(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－265361
(P2001－265361A)
(43)公開日　平成13年９月28日(2001.9.28)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | テーマコード(参考) |
|---|---|---|---|
| Ｇ１０Ｋ　15/04 | ３０２ | Ｇ１０Ｋ　15/04 | ３０２Ｂ　５Ｊ１０４ |
| Ｈ０４Ｌ　9/08 | | Ｈ０４Ｌ　9/00 | ６０１Ｂ |

審査請求　未請求　請求項の数７　ＯＬ　（全 34 頁）

(21)出願番号　特願2000－70461(P2000－70461)

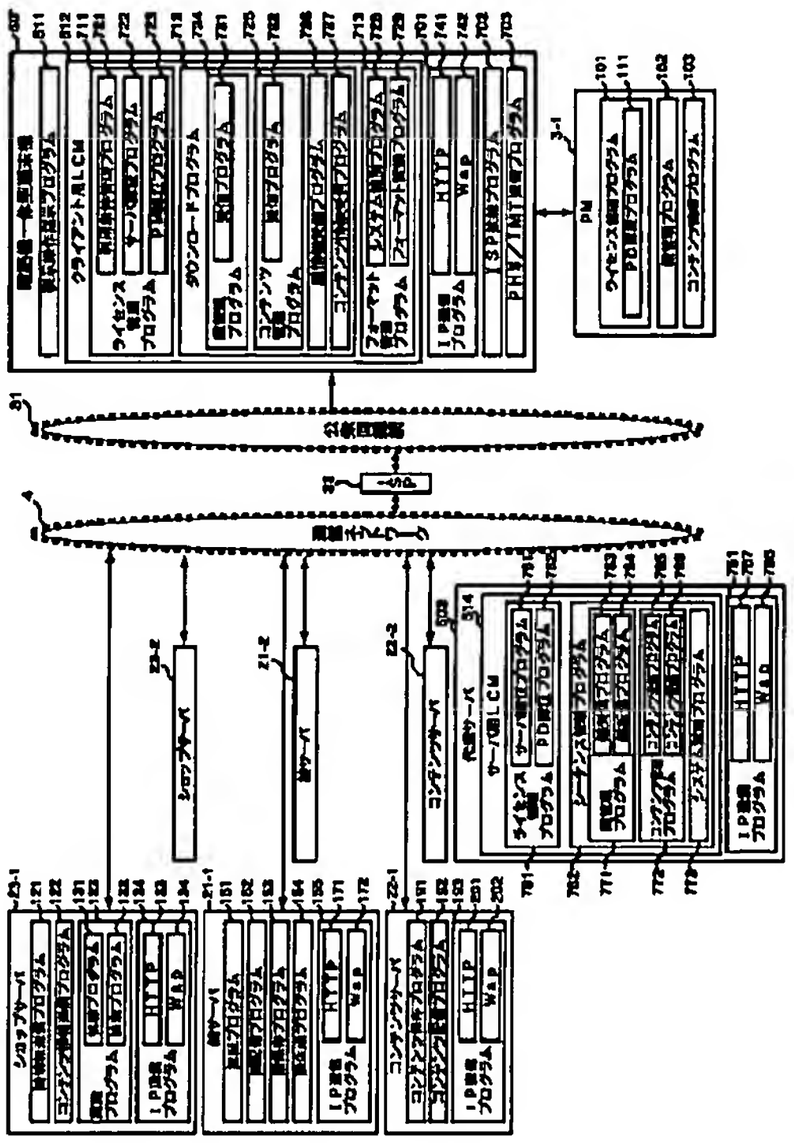
(22)出願日　平成12年３月14日(2000.3.14)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　郷　直美
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　栗原　章
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

Ｆターム(参考)　5J104 AA01 AA16 EA01 EA04 EA16 NA02 PA07

(54)【発明の名称】　情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体

(57)【要約】
【課題】　異なる手順で供給されるコンテンツおよび鍵を受信する。
【解決手段】　ライセンス管理プログラム７６１は、電話機一体型端末機５０１を認証するとともに、第１のサーバまたは第２のサーバを認証する。サーバ用ＬＣＭ５１４は、コンテンツおよび鍵の送信要求、並びに第１のサーバを特定するデータまたは第２のサーバを特定するデータの受信を制御して、第１のサーバを特定するデータを受信した場合、第１のサーバに対応する手続で、第１のサーバからコンテンツおよび鍵を受信し、第２のサーバを特定するデータを受信した場合、第２のサーバに対応する手続で、第２のサーバからコンテンツおよび鍵を受信するように通信を制御する。サーバ用ＬＣＭ５１４は、電話機一体型端末機５０１へのコンテンツおよび鍵の送信を制御する。



【特許請求の範囲】
【請求項１】　第１の情報処理装置を認証する第１の認証手段と、
第２の情報処理装置または第３の情報処理装置を認証する第２の認証手段と、
前記第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第２の情報処理装置を特定するデータまたは前記第３の情報処理装置を特定するデータの受信を制御する受信制御手段と、
前記第２の情報処理装置を特定する前記データを受信した場合、前記第２の情報処理装置に対応した手順で、前記第２の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第２の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第３の情報処理装置を特定する前記データを受信した場合、前記第３の情報処理装置に対応した手順で、前記第３の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第３の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御手段と、
前記第１の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御手段とを含むことを特徴とする情報提供装置。
【請求項２】　前記コンテンツの符号化方式および暗号化方式のうちの少なくとも一方を、所定の符号化方式または暗号化方式に変換する変換手段を更に含むことを特徴とする請求項１に記載の情報提供装置。
【請求項３】　第１の情報処理装置を認証する第１の認証ステップと、
第２の情報処理装置または第３の情報処理装置を認証する第２の認証ステップと、
前記第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第２の情報処理装置を特定するデータまたは前記第３の情報処理装置を特定するデータの受信を制御する受信制御ステップと、
前記第２の情報処理装置を特定する前記データを受信した場合、前記第２の情報処理装置に対応した手順で、前記第２の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第２の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第３の情報処理装置を特定する前記データを受信した場合、前記第３の情報処理装置に対応した手順で、前記第３の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第３の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御ステップと、
前記第１の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御ステップとを含むことを特徴とする情報提供方法。
【請求項４】　第１の情報処理装置を認証する第１の認証ステップと、
第２の情報処理装置または第３の情報処理装置を認証する第２の認証ステップと、
前記第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第２の情報処理装置を特定するデータまたは前記第３の情報処理装置を特定するデータの受信を制御する受信制御ステップと、
前記第２の情報処理装置を特定する前記データを受信した場合、前記第２の情報処理装置に対応した手順で、前記第２の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第２の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第３の情報処理装置を特定する前記データを受信した場合、前記第３の情報処理装置に対応した手順で、前記第３の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第３の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御ステップと、
前記第１の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。
【請求項５】　第１の情報提供装置を認証する認証手段と、
前記第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する第２の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御手段と、
前記第２の情報提供装置または前記第３の情報提供装置から前記第１の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御手段とを含むことを特徴とする情報処理装置。
【請求項６】　第１の情報提供装置を認証する認証ステップと、
前記第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する第２の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、
前記第２の情報提供装置または前記第３の情報提供装置から前記第１の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御ステップとを含むことを特徴とする情報処理方法。
【請求項７】　第１の情報提供装置を認証する認証ステップと、
前記第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する

第２の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、
前記第２の情報提供装置または前記第３の情報提供装置から前記第１の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体に関し、特に、コンテンツおよびコンテンツを復号する鍵を提供するか、または暗号化されているコンテンツを利用する情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体に関する。
【０００２】
【従来の技術】図１は、従来のデジタルデータ伝送システムの構成を示す図である。パーソナルコンピュータ１は、ローカルエリアネットワークまたはインターネットなどから構成される通信ネットワーク４に接続されている。パーソナルコンピュータ１は、コンテンツサーバ２２－１若しくは２２－２から受信した、またはCD（Compact Disc）から読み取った楽音のデータ（以下、コンテンツと称する）を、所定の圧縮の方式（例えば、ATRAC3（商標））に変換するとともにDES（Data Encryption Standard）などの暗号化方式で暗号化して記録する。
【０００３】パーソナルコンピュータ１は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。
【０００４】利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に利用することができるポータブルデバイス（Portable Device（PDとも称する））の台数（後述する、いわゆるチェックアウトできるPDの台数）を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ１は、そのコンテンツを再生できる。
【０００５】パーソナルコンピュータ１の表示操作指示プログラム１１は、パーソナルコンピュータ１が記録しているコンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、チェックアウトの指示などを入力して、ＳＤＭＩ（Secure Digital Music Initiative）の規格に準拠したソフトウェアモジュールであるＬＣＭ（Licensed Compliant Module）１２にその指示に対応したチェックアウトなどの処理を実行させる。
【０００６】パーソナルコンピュータ１のＬＣＭ１２は、コンテンツの不正な２次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。
【０００７】ＬＣＭ１２は、パーソナルコンピュータ１に接続された機器が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、ＬＣＭ１２は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との通信を制御する。
【０００８】また、ＬＣＭ１２は、装着されているポータブルメディア３の正当性をチェックして、サーバ５が指定した利用条件をコンテンツ（暗号化されている）に付加して、コンテンツを記録させる。
【０００９】パーソナルコンピュータ１のＬＣＭ１２は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ（例えば、曲名、または利用条件など）と共に、接続されているポータブルデバイス２に供給するとともに、ポータブルデバイス２に供給したことに対応して、供給したコンテンツに対応する利用条件のデータを更新する（以下、チェックアウトと称する）。より詳細には、チェックアウトしたとき、パーソナルコンピュータ１が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、１減らされる。チェックアウトできる回数が０のとき、対応するコンテンツは、チェックアウトすることができない。
【００１０】ポータブルデバイス２は、パーソナルコンピュータ１から供給されたコンテンツ（すなわち、チェックアウトされたコンテンツ）を、コンテンツに関連するデータ（例えば、曲名、または利用条件など）と共に、装着されているポータブルメディア３に記憶させる。
【００１１】ポータブルメディア３は、フラッシュメモリなどの記憶媒体をその内部に有し、ポータブルデバイス２に着脱可能に構成されている。
【００１２】ポータブルデバイス２は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア３に記憶されているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。
【００１３】例えば、コンテンツに関連する利用条件のデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス２は、対応するコンテンツの再生を停止する。
【００１４】使用者は、コンテンツを記憶したポータブルデバイス２をパーソナルコンピュータ１から取り外して、持ち歩き、ポータブルメディア３に記憶されているコンテンツを再生させて、コンテンツに対応する音楽な

どをヘッドフォンなどで聴くことができる。
【００１５】ポータブルデバイス２がUSBケーブル等を介してパーソナルコンピュータ１に接続されたとき、ポータブルデバイス２とパーソナルコンピュータ１とは、相互認証の処理を実行する。この相互認証の処理は、チャレンジレスポンス方式の認証の処理である。チャレンジレスポンス方式とは、パーソナルコンピュータ１が生成するある値（チャレンジ）に対して、ポータブルデバイス２がパーソナルコンピュータ１と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。
【００１６】サーバ５－１は、所定の方式で圧縮符号化され、暗号化されたコンテンツを蓄積して、パーソナルコンピュータ１からの要求に対応して蓄積しているコンテンツを配信する。サーバ５－１は、鍵サーバ２１－１、コンテンツサーバ２２－１、およびショップサーバ２３－１の機能を有する。
【００１７】鍵サーバ２１－１は、コンテンツサーバ２２－１がパーソナルコンピュータ１に供給したコンテンツを復号するためのコンテンツ鍵を蓄積し、パーソナルコンピュータ１の要求に対応して、コンテンツ鍵をパーソナルコンピュータ１に供給する。コンテンツ鍵の供給の前に、鍵サーバ２１－１とパーソナルコンピュータ１とは、相互認証の処理を実行して、鍵サーバ２１－１は、その相互認証の処理により共有された一時鍵でコンテンツ鍵を暗号化して、パーソナルコンピュータ１に送信する。パーソナルコンピュータ１は、受信したコンテンツ鍵を共有している一時鍵で復号する。
【００１８】コンテンツサーバ２２－１は、パーソナルコンピュータ１の要求に対応して、通信ネットワーク４を介して、パーソナルコンピュータ１に、コンテンツに対応する利用条件と共にコンテンツ（暗号化されている）を供給する。
【００１９】ショップサーバ２３－１は、コンテンツサーバ２２－１が供給するコンテンツに関連するデジタルデータ（コンテンツの曲名、価格などを含むコンテンツの一覧などを含む）をパーソナルコンピュータ１に提供するとともに、パーソナルコンピュータ１からのコンテンツの購入の申し込みに対応して、そのコンテンツを供給するコンテンツサーバ２２－１のＵＲＬ（Uniform Resource Locator）、およびそのコンテンツを復号するコンテンツ鍵を供給する鍵サーバ２１－１のＵＲＬなどをパーソナルコンピュータ１に供給する。
【００２０】サーバ５－２は、所定の方式で圧縮符号化され、暗号化されたコンテンツを蓄積して、パーソナルコンピュータ１からの要求に対応して蓄積しているコンテンツを配信する。サーバ５－２は、鍵サーバ２１－２、コンテンツサーバ２２－２、およびショップサーバ２３－２の機能を有する。
【００２１】鍵サーバ２１－２は、コンテンツサーバ２－２がパーソナルコンピュータ１に供給したコンテンツを復号するためのコンテンツ鍵を蓄積し、パーソナルコンピュータ１の要求に対応して、コンテンツ鍵をパーソナルコンピュータ１に供給する。コンテンツ鍵の供給の前に、鍵サーバ２１－２とパーソナルコンピュータ１とは、相互認証の処理を実行して、鍵サーバ２１－２は、その相互認証の処理により共有された一時鍵でコンテンツ鍵を暗号化して、パーソナルコンピュータ１に送信する。パーソナルコンピュータ１は、受信したコンテンツ鍵を共有している一時鍵で復号する。
【００２２】コンテンツサーバ２２－２は、パーソナルコンピュータ１の要求に対応して、通信ネットワーク４を介して、パーソナルコンピュータ１に、コンテンツに対応する利用条件と共にコンテンツ（暗号化されている）を供給する。
【００２３】ショップサーバ２３－２は、コンテンツサーバ２２－２が供給するコンテンツに関連するデジタルデータ（コンテンツの曲名、価格などを含むコンテンツの一覧などを含む）をパーソナルコンピュータ１に提供するとともに、パーソナルコンピュータ１からのコンテンツの購入の申し込みに対応して、そのコンテンツを供給するコンテンツサーバ２２－２のＵＲＬ、およびそのコンテンツを復号するコンテンツ鍵を供給する鍵サーバ２１－２のＵＲＬなどをパーソナルコンピュータ１に供給する。
【００２４】以下、サーバ５－１およびサーバ５－２を個々に区別する必要がないとき、単に、サーバ５と称する。以下、鍵サーバ２１－１および鍵サーバ２１－２を個々に区別する必要がないとき、単に、鍵サーバ２１と称する。以下、コンテンツサーバ２２－１およびコンテンツサーバ２２－２を個々に区別する必要がないとき、単に、コンテンツサーバ２２と称する。以下、ショップサーバ２３－１およびショップサーバ２３－２を個々に区別する必要がないとき、単に、ショップサーバ２３と称する。
【００２５】次に、図２を参照して、従来のデジタルデータ伝送システムの機能の構成について説明する。パーソナルコンピュータ１は、表示操作指示プログラム１１およびＬＣＭ１２に加えて、ＩＰ（Internet Protocol）通信プログラム１３、ＩＳＰ（Internet Service Provider）接続プログラム１４、およびＰＨＳ（Personal Handyphone System）／ＩＭＴ（International Mobile Telecommunication System）通信プログラム１５を実行する。
【００２６】ＰＨＳ／ＩＭＴ通信プログラム１５は、公衆回線網３１を介して通信を行うためのプログラムである。ＩＳＰ接続プログラム１４は、ＩＳＰ３２と接続するためのプログラムである。ＩＰ通信プログラム１３は、ＨＴＴＰ（Hypertext Transport Protocol）７４およびＷａｐ（Wireless Access Protocol）７５などの手

続を包含し、通信ネットワーク４を介して、鍵サーバ２１、コンテンツサーバ２２、またはショップサーバ２３と通信するためのプログラムである。

【００２７】ＬＣＭ１２は、ライセンス管理プログラム５１、ダウンロードプログラム５２－１、ダウンロードプログラム５２－２、およびフォーマット管理プログラム５３から構成されている。

【００２８】ライセンス管理プログラム５１は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム６１、CDリッピングプログラム６２、およびPD認証プログラム６３から構成されている。

【００２９】利用条件管理プログラム６１は、コンテンツの利用条件に基づいて、パーソナルコンピュータ１が記録しているコンテンツのチェックアウトなどを許可するか、または禁止するかなどの管理を実行するとともに、コンテンツのチェックアウトなどに対応して利用条件のデータを更新する。CDリッピングプログラム６２は、パーソナルコンピュータ１に装着されたCDからコンテンツを読み出すとともに、読み出したコンテンツに対応する利用条件を生成する。

【００３０】PD認証プログラム６３は、パーソナルコンピュータ１に装着されているポータブルデバイス２を認証する。

【００３１】ダウンロードプログラム５２－１は、サーバ５－１からコンテンツおよびコンテンツ鍵をダウンロードするためのプログラムであり、鍵管理プログラム６４、コンテンツ管理プログラム６５、鍵情報受信プログラム６６、およびコンテンツ情報受信プログラム６７から構成されている。

【００３２】鍵管理プログラム６４は、鍵サーバ２１－１の認証の処理を実行して、鍵サーバ２１－１からコンテンツ鍵を受信して、コンテンツに対応させてコンテンツ鍵を管理する。鍵管理プログラム６４は、サーバ認証プログラム７１および受信プログラム７２から構成される。

【００３３】サーバ認証プログラム７１は、後述する処理により、鍵サーバ２１－１を認証する。受信プログラム７２は、通信ネットワーク４を介して、鍵サーバ２１－１からコンテンツ鍵を受信する。

【００３４】コンテンツ管理プログラム６５は、通信ネットワーク４を介して、コンテンツサーバ２２－１からコンテンツの利用条件のデータとともにコンテンツを受信して、コンテンツの利用条件のデータとともにコンテンツを記録する。コンテンツ管理プログラム６５の受信プログラム７３は、コンテンツサーバ２２－１からコンテンツの利用条件のデータおよびコンテンツを受信する。

【００３５】鍵情報受信プログラム６６は、ショップサーバ２３－１から、所望のコンテンツに対応するコンテンツ鍵を供給する鍵サーバ２１－１を特定するＵＲＬを受信する。コンテンツ情報受信プログラム６７は、ショップサーバ２３－１から、使用者が所望するコンテンツを特定するコンテンツＩＤ、およびそのコンテンツを供給するコンテンツサーバ２２－１を特定するＵＲＬを受信する。

【００３６】ダウンロードプログラム５２－２は、サーバ５－２からコンテンツおよびコンテンツ鍵をダウンロードするためのプログラムであり、ダウンロードプログラム５２－１と同様の構成を有するので、その説明は省略する。

【００３７】フォーマット管理プログラム５３は、コンテンツサーバ２２－１または２２－２からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換するとともに、CDから読み出したコンテンツを所定の方式で符号化して暗号化する。フォーマット管理プログラム５３は、システム識別プログラム６８およびフォーマット変換プログラム６９から構成されている。

【００３８】システム識別プログラム６８は、コンテンツのダウンロード先が、サーバ５－１であるか、サーバ５－２であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム６９は、コンテンツの符号化方式および暗号化方式を変換する。

【００３９】ポータブルデバイス２は、ライセンス管理プログラム８１、鍵管理プログラム８２、およびコンテンツ管理プログラム８３を実行する。

【００４０】ライセンス管理プログラム８１は、コンテンツに対応する利用条件を基に、コンテンツの再生の回数などを管理する利用条件管理プログラム９１、パーソナルコンピュータ１を認証するPC認証プログラム９２、およびポータブルメディア３を認証するPM認証プログラム９３から構成される。

【００４１】鍵管理プログラム８２は、パーソナルコンピュータ１から供給されたコンテンツ鍵を、ポータブルメディア３が予め記憶している保存用鍵で暗号化させ、ポータブルメディア３に記憶させて管理する。

【００４２】コンテンツ管理プログラム８３は、パーソナルコンピュータ１から供給されたコンテンツを、ポータブルメディア３に記憶させて管理する。

【００４３】ポータブルメディア３は、ライセンス管理プログラム１０１、鍵管理プログラム１０２、およびコンテンツ管理プログラム１０３を実行する。

【００４４】ライセンス管理プログラム１０１は、ポータブルデバイス２を認証するPD認証プログラム１１１を有し、コンテンツに対応する利用条件のデータを記憶して、利用条件のデータに基づいて、コンテンツの読み出し等を制御する。鍵管理プログラム１０２は、ポータブルデバイス２から供給されたコンテンツ鍵を、予め記憶している保存用鍵で暗号化して記憶し、管理する。コン

テンツ管理プログラム１０３は、ポータブルデバイス２から供給されたコンテンツを記憶して、管理する。

【００４５】ショップサーバ２３－１は、鍵情報送信プログラム１２１、コンテンツ情報送信プログラム１２２、閲覧プログラム１２３、およびＩＰ通信プログラム１２４を実行する。

【００４６】鍵情報送信プログラム１２１は、通信ネットワーク４を介して、パーソナルコンピュータ１に、パーソナルコンピュータ１の使用者が所望するコンテンツに対応するコンテンツ鍵を供給する鍵サーバ２１－１のＵＲＬを送信する。

【００４７】コンテンツ情報送信プログラム１２２は、通信ネットワーク４を介して、パーソナルコンピュータ１に、パーソナルコンピュータ１の使用者が所望するコンテンツを供給するコンテンツサーバ２２－１のＵＲＬを送信する。

【００４８】閲覧プログラム１２３は、コンテンツをパーソナルコンピュータ１の使用者に視聴させる視聴プログラム１３１、およびパーソナルコンピュータ１の使用者が所望のコンテンツを検索する検索プログラム１３２から構成されている。

【００４９】ＩＰ通信プログラム１２４は、ＨＴＴＰ１３３およびＷａｐ１３４などの手続を包含し、通信ネットワーク４を介して、パーソナルコンピュータ１と通信するためのプログラムである。

【００５０】鍵サーバ２１－１は、認証プログラム１５１、鍵配信プログラム１５２、鍵保存プログラム１５３、鍵生成プログラム１５４、およびＩＰ通信プログラム１５５を実行する。

【００５１】認証プログラム１５１は、パーソナルコンピュータ１などを認証するプログラムである。鍵配信プログラム１５２は、認証されたパーソナルコンピュータ１に、鍵保存プログラム１５３が保存しているコンテンツ鍵を配信するプログラムである。鍵保存プログラム１５３は、鍵生成プログラム１５４により生成されたコンテンツ鍵を保存するプログラムである。鍵生成プログラム１５４は、コンテンツに対応させてコンテンツ鍵を生成するプログラムである。

【００５２】ＩＰ通信プログラム１５５は、ＨＴＴＰ１７１およびＷａｐ１７２などの手続を包含し、通信ネットワーク４を介して、パーソナルコンピュータ１などと通信するためのプログラムである。

【００５３】コンテンツサーバ２２－１は、コンテンツ保存プログラム１９１、コンテンツ配信プログラム１９２、およびＩＰ通信プログラム１９３を実行する。

【００５４】コンテンツ保存プログラム１９１は、暗号化されているコンテンツをコンテンツＩＤと対応させて保存する。コンテンツ配信プログラム１９２は、パーソナルコンピュータ１から要求があったとき、コンテンツ保存プログラム１９１が保存している、コンテンツＩＤに対応するコンテンツをパーソナルコンピュータ１に配信する。

【００５５】ＩＰ通信プログラム１９３は、ＨＴＴＰ２０１およびＷａｐ２０２などの手続を包含し、通信ネットワーク４を介して、パーソナルコンピュータ１と通信するためのプログラムである。

【００５６】ショップサーバ２３－２は、ショップサーバ２３－１と同様の構成を有するので、その説明は省略する。鍵サーバ２１－２は、鍵サーバ２１－１と同様の構成を有するので、その説明は省略する。コンテンツサーバ２２－２は、コンテンツサーバ２２－１と同様の構成を有するのでその説明は省略する。

【００５７】次に、パーソナルコンピュータ１がサーバ５－１からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする従来の処理を図３および図４のフローチャートを参照して説明する。ステップＳ１０１において、パーソナルコンピュータ１のＰＨＳ／ＩＭＴ通信プログラム１５は、公衆回線網３１と接続を確立する。ステップＳ２０１において、公衆回線網３１の図示せぬ地上局などは、パーソナルコンピュータ１と接続を確立する。

【００５８】ステップＳ１０２において、パーソナルコンピュータ１のＩＳＰ接続プログラム１４は、ＩＳＰ３２と接続を確立する。ステップＳ３０１において、ＩＳＰ３２は、パーソナルコンピュータ１と接続を確立する。

【００５９】ステップＳ１０３において、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ショップサーバ２３とＩＰ通信を確立する。ステップＳ４０１において、ショップサーバ２３－１のＩＰ通信プログラム１２４は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００６０】ステップＳ４０２において、ショップサーバ２３－１の閲覧プログラム１２３は、通信ネットワーク４を介して、パーソナルコンピュータ１に閲覧用（コンテンツの選択用）のデジタルデータを送信する。ステップＳ１０４において、パーソナルコンピュータ１の図示せぬブラウザプログラムは、デジタルデータに対応する画像またはテキストなどを表示し、使用者に閲覧させる。また、パーソナルコンピュータ１のブラウザプログラムは、コンテンツのストリーミング再生によりコンテンツを使用者に試聴させたり、または、キーワードによりコンテンツをショップサーバ２３－１の閲覧プログラム１２３に検索させ、その結果を表示する。ステップＳ４０２およびステップＳ１０４の処理は、パーソナルコンピュータ１の使用者の要求に対応して、繰り返される。

【００６１】ステップＳ１０５において、パーソナルコンピュータ１のブラウザプログラムは、購入依頼をショップサーバ２３－１に送信する。ステップＳ４０３にお

いて、ショップサーバ２３－１の閲覧プログラム１２３は、パーソナルコンピュータ１から送信された購入依頼を受信する。

【００６２】ステップＳ４０４において、ショップサーバ２３－１のコンテンツ情報送信プログラム１２２は、ステップＳ４０３の処理で受信した購入依頼に対応するコンテンツを配信するコンテンツサーバ２２－１のＵＲＬおよびコンテンツを特定するためのコンテンツＩＤなどを含む、コンテンツ情報を通信ネットワーク４を介してパーソナルコンピュータ１に送信する。ステップＳ１０６において、パーソナルコンピュータ１のコンテンツ情報受信プログラム６７は、ショップサーバ２３－１が送信した、コンテンツ情報を受信する。

【００６３】ステップＳ４０５において、ショップサーバ２３－１の鍵情報送信プログラム１２１は、ステップＳ４０３の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ２１－１のＵＲＬなどの、鍵情報を通信ネットワーク４を介してパーソナルコンピュータ１に送信する。ステップＳ１０７において、パーソナルコンピュータ１の鍵情報受信プログラム６６は、ショップサーバ２３－１が送信した鍵情報を受信する。

【００６４】ステップＳ１０８において、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ステップＳ１０６の処理で取得したコンテンツ情報に含まれるコンテンツサーバ２２－１のＵＲＬを基に、コンテンツサーバ２２－１とＩＰ通信を確立する。ステップＳ５０１において、コンテンツサーバ２２－１のＩＰ通信プログラム１９３は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００６５】ステップＳ１０９において、パーソナルコンピュータ１のコンテンツ管理プログラム６５は、ステップＳ１０６の処理で取得したコンテンツＩＤを、通信ネットワーク４を介して、コンテンツサーバ２２－１に送信する。ステップＳ５０２において、コンテンツサーバ２２－１は、パーソナルコンピュータ１が送信したコンテンツＩＤを受信する。ステップＳ５０３において、コンテンツサーバ２２－１のコンテンツ配信プログラム１９２は、ステップＳ５０２で受信したコンテンツＩＤに対応するコンテンツ（暗号化されている）をコンテンツ保存プログラム１９１から読み出して、通信ネットワーク４を介して、パーソナルコンピュータ１に配信する。ステップＳ１１０において、パーソナルコンピュータ１のコンテンツ管理プログラム６５の受信プログラム７３は、コンテンツサーバ２２－１が送信したコンテンツを受信する。

【００６６】ステップＳ１１１において、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ステップＳ１０７の処理で取得した鍵情報に含まれる鍵サーバ２１－１のＵＲＬを基に、鍵サーバ２１－１とＩＰ通信を確立する。ステップＳ６０１において、鍵サーバ２１－１のＩＰ通信プログラム１５５は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００６７】ステップＳ１１２において、パーソナルコンピュータ１の鍵管理プログラム６４のサーバ認証プログラム７１は、鍵サーバ２１－１を認証する。ステップＳ６０２において、鍵サーバ２１－１の認証プログラム１５１は、パーソナルコンピュータ１を認証する。

【００６８】鍵サーバ２１－１には、マスター鍵ＫMSが予め記憶されており、パーソナルコンピュータ１には、個別鍵ＫPPとパーソナルコンピュータ１のIDが予め記憶されている。パーソナルコンピュータ１には、更に、マスター鍵ＫMPが予め記憶されており、鍵サーバ２１－１にも鍵サーバ２１－１のIDと個別鍵ＫPSが記憶されている。

【００６９】鍵サーバ２１－１は、パーソナルコンピュータ１から、パーソナルコンピュータ１のIDの供給を受け、そのIDと自分自身が有するマスター鍵ＫMSにハッシュ関数を適用して、パーソナルコンピュータ１の個別鍵ＫPPと同一の鍵を生成する。

【００７０】パーソナルコンピュータ１は、鍵サーバ２１－１から、鍵サーバ２１－１のIDの供給を受け、そのIDと自分自身が有するマスター鍵ＫMPにハッシュ関数を適用して、鍵サーバ２１－１の個別鍵ＫPSと同一の鍵を生成する。このようにすることで、パーソナルコンピュータ１と鍵サーバ２１－１の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時鍵を生成する。

【００７１】ステップＳ１１３において、パーソナルコンピュータ１の鍵管理プログラム６４は、コンテンツＩＤを鍵サーバ２１－１に送信する。ステップＳ６０３において、鍵サーバ２１－１は、パーソナルコンピュータ１が送信した、コンテンツＩＤを受信する。ステップＳ６０４において、鍵サーバ２１－１の鍵配信プログラム１５２は、鍵保存プログラム１５３がコンテンツＩＤと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク４を介して、そのコンテンツ鍵（一時鍵により暗号化されている）をパーソナルコンピュータ１に送信する。ステップＳ１１４において、パーソナルコンピュータ１の鍵管理プログラム６４の受信プログラム７２は、鍵サーバ２１－１が送信したコンテンツ鍵を受信する。鍵管理プログラム６４は、受信したコンテンツ鍵を一時鍵で復号する。

【００７２】ステップＳ１１５において、パーソナルコンピュータ１のＰＨＳ／ＩＭＴ通信プログラム１５は、公衆回線網３１との接続を切断する。ステップＳ２０２において、公衆回線網３１の図示せぬ地上局などは、パーソナルコンピュータ１との接続を切断する。

【００７３】ステップＳ１１６において、フォーマット管理プログラム５３は、ステップＳ１１０の処理で受信

したコンテンツの符号化方式および暗号化方式を、それぞれ所定の方式に変換する。

【００７４】パーソナルコンピュータ１の使用者が、表示操作指示プログラム１１に対し、受信したコンテンツのチェックアウトを指示したとき、ステップＳ１１７以降の処理が実行される。

【００７５】ステップＳ１１７において、パーソナルコンピュータ１のライセンス管理プログラム５１のPD認証プログラム６３は、ポータブルデバイス２を認証する。ステップＳ７０１において、ポータブルデバイス２のライセンス管理プログラム８１のPC認証プログラム９２は、パーソナルコンピュータ１を認証する。

【００７６】ステップＳ１１７およびステップＳ７０１におけるパーソナルコンピュータ１とポータブルデバイス２との相互認証の処理は、チャレンジレスポンス方式の認証の処理であり、ステップＳ１１２およびステップＳ６０２における鍵サーバ２１－１とパーソナルコンピュータ１との相互認証の処理に比較して、演算量が少ない。パーソナルコンピュータ１およびポータブルデバイス２は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

【００７７】ステップＳ１１８において、パーソナルコンピュータ１のコンテンツ管理プログラム６５は、暗号化されているコンテンツをポータブルデバイス２に配信する。ステップＳ７０２において、ポータブルデバイス２のコンテンツ管理プログラム８３は、パーソナルコンピュータ１が配信したコンテンツを受信して、ポータブルメディア３のコンテンツ管理プログラム１０３に供給する。ポータブルメディア３のコンテンツ管理プログラム１０３は、コンテンツを記憶する。

【００７８】なお、ポータブルデバイス２とポータブルメディア３は、ポータブルデバイス２にポータブルメディア３が装着されたとき、相互認証する。

【００７９】ステップＳ１１９において、パーソナルコンピュータ１の鍵管理プログラム６４は、ポータブルデバイス２に、ステップＳ１１８で配信したコンテンツに対応するコンテンツ鍵（ポータブルデバイス２とポータブルメディア３とで共有する一時鍵で暗号化されている）を配信する。ステップＳ７０３において、ポータブルデバイス２の鍵管理プログラム８２は、パーソナルコンピュータ１が配信したコンテンツ鍵を受信して、ポータブルメディア３の鍵管理プログラム１０２に供給する。ポータブルメディア３の鍵管理プログラム１０２は、コンテンツ鍵を一時鍵で復号して、コンテンツ鍵を記憶する。

【００８０】次に、パーソナルコンピュータ１がサーバ５－２からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする処理を図５および図６のフローチャートを参照して説明する。ステップＳ１１０１乃至ステップＳ１１０７の処理は、サーバ５－２、並びにＩＰ通信プログラム１３、ＩＳＰ接続プログラム１４、ＰＨＳ／ＩＭＴ通信プログラム１５、およびダウンロードプログラム５２－２により実行され、それぞれ、ステップＳ１０１乃至ステップＳ１０７の処理と同様なので、その説明は省略する。

【００８１】ステップＳ１１０８において、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ステップＳ１１０７の処理で取得した鍵情報に含まれる鍵サーバ２１－２のＵＲＬを基に、鍵サーバ２１－２とＩＰ通信を確立する。ステップＳ１６０１において、鍵サーバ２１－２は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００８２】ステップＳ１１０９において、パーソナルコンピュータ１のダウンロードプログラム５２－２は、鍵サーバ２１－２を認証する。ステップＳ１６０２において、鍵サーバ２１－２は、パーソナルコンピュータ１を認証する。ステップＳ１１０９およびステップＳ１６０２の処理は、ステップＳ１１２およびステップＳ６０２の処理と同様の処理である。

【００８３】ステップＳ１１１０において、パーソナルコンピュータ１のダウンロードプログラム５２－２は、コンテンツＩＤを鍵サーバ２１－２に送信する。ステップＳ１６０３において、鍵サーバ２１－２は、パーソナルコンピュータ１が送信した、コンテンツＩＤを受信する。ステップＳ１６０４において、鍵サーバ２１－２は、コンテンツＩＤと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク４を介して、そのコンテンツ鍵（一時鍵により暗号化されている）をパーソナルコンピュータ１に送信する。ステップＳ１１１１において、パーソナルコンピュータ１のダウンロードプログラム５２－２は、鍵サーバ２１－２が送信したコンテンツ鍵を受信する。ダウンロードプログラム５２－２は、受信したコンテンツ鍵を一時鍵で復号する。

【００８４】ステップＳ１１１２おいて、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ステップＳ１１０６の処理で取得したコンテンツ情報に含まれるコンテンツサーバ２２－２のＵＲＬを基に、コンテンツサーバ２２－２とＩＰ通信を確立する。ステップＳ１５０１において、コンテンツサーバ２２－２は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００８５】ステップＳ１１１３において、パーソナルコンピュータ１のダウンロードプログラム５２－２は、ステップＳ１１０６の処理で取得したコンテンツＩＤを、通信ネットワーク４を介して、コンテンツサーバ２２－２に送信する。ステップＳ１５０２において、コンテンツサーバ２２－２は、パーソナルコンピュータ１が送信したコンテンツＩＤを受信する。ステップＳ１５０３において、コンテンツサーバ２２－２は、ステップＳ１５０２で受信したコンテンツＩＤに対応するコンテンツ（暗号化されている）を読み出して、通信ネットワー

ク４を介して、パーソナルコンピュータ１に配信する。ステップＳ１１１４において、パーソナルコンピュータ１のダウンロードプログラム５２－２は、コンテンツサーバ２２－２が送信したコンテンツを受信する。

【００８６】ステップＳ１１１５乃至ステップＳ１７０３の処理は、ステップＳ１１５乃至ステップＳ７０３の処理と同様なので、その説明は省略する。

【００８７】

【発明が解決しようとする課題】以上のように、コンテンツおよびコンテンツ鍵を供給するサーバ５－１または５－２は、それぞれ、コンテンツおよびコンテンツ鍵を供給する手順が異なるので、サーバ５－１および５－２からのコンテンツの受信を所望する場合、サーバ５－１に対応するダウンロードプログラム５２－１とサーバ５－２に対応するダウンロードプログラム５２－２とが必要となる。

【００８８】しかしながら、コンテンツを受信する装置の、演算能力が小さい、記憶容量が少ないなどの処理能力が小さい場合、コンテンツを受信する装置は、複数のダウンロードプログラムを記憶しておくことができず、ダウンロードプログラムを切り換えて実行することができない。

【００８９】本発明はこのような状況に鑑みてなされたものであり、処理能力が小さい装置でも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようにすることを目的とする。

【００９０】

【課題を解決するための手段】請求項１に記載の情報提供装置は、第１の情報処理装置を認証する第１の認証手段と、第２の情報処理装置または第３の情報処理装置を認証する第２の認証手段と、第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第２の情報処理装置を特定するデータまたは第３の情報処理装置を特定するデータの受信を制御する受信制御手段と、第２の情報処理装置を特定するデータを受信した場合、第２の情報処理装置に対応した手順で、第２の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第２の情報処理装置からコンテンツおよび鍵を受信し、第３の情報処理装置を特定するデータを受信した場合、第３の情報処理装置に対応した手順で、第３の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第３の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御手段と、第１の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御手段とを含むことを特徴とする。

【００９１】情報提供装置は、コンテンツの符号化方式および暗号化方式のうちの少なくとも一方を、所定の符号化方式または暗号化方式に変換する変換手段を更に設けことかできる。

【００９２】請求項３に記載の情報提供方法は、第１の情報処理装置を認証する第１の認証ステップと、第２の情報処理装置または第３の情報処理装置を認証する第２の認証ステップと、第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第２の情報処理装置を特定するデータまたは第３の情報処理装置を特定するデータの受信を制御する受信制御ステップと、第２の情報処理装置を特定するデータを受信した場合、第２の情報処理装置に対応した手順で、第２の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第２の情報処理装置からコンテンツおよび鍵を受信し、第３の情報処理装置を特定するデータを受信した場合、第３の情報処理装置に対応した手順で、第３の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第３の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御ステップと、第１の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

【００９３】請求項４に記載のプログラム格納媒体のプログラムは、第１の情報処理装置を認証する第１の認証ステップと、第２の情報処理装置または第３の情報処理装置を認証する第２の認証ステップと、第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第２の情報処理装置を特定するデータまたは第３の情報処理装置を特定するデータの受信を制御する受信制御ステップと、第２の情報処理装置を特定するデータを受信した場合、第２の情報処理装置に対応した手順で、第２の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第２の情報処理装置からコンテンツおよび鍵を受信し、第３の情報処理装置を特定するデータを受信した場合、第３の情報処理装置に対応した手順で、第３の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第３の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御ステップと、第１の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

【００９４】請求項５に記載の情報処理装置は、第１の情報提供装置を認証する認証手段と、第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第２の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御手段と、第２の情報提供装置または第３の情報提供装置から第１の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信を制御する受信制御手段とを含むことを特徴とする。

【００９５】請求項６に記載の情報処理方法は、第１の情報提供装置を認証する認証ステップと、第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第２の情報提供装置を特定

するデータ、およびコンテンツおよび鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、第２の情報提供装置または第３の情報提供装置から第１の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

【００９６】請求項７に記載のプログラム格納媒体のプログラムは、第１の情報提供装置を認証する認証ステップと、第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第２の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、第２の情報提供装置または第３の情報提供装置から第１の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

【００９７】請求項１に記載の情報提供装置、請求項３に記載の情報提供方法、および請求項４に記載のプログラム格納媒体においては、第１の情報処理装置が認証され、第２の情報処理装置または第３の情報処理装置が認証され、第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第２の情報処理装置を特定するデータまたは第３の情報処理装置を特定するデータの受信が制御され、第２の情報処理装置を特定するデータを受信した場合、第２の情報処理装置に対応した手順で、第２の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第２の情報処理装置からコンテンツおよび鍵を受信し、第３の情報処理装置を特定するデータを受信した場合、第３の情報処理装置に対応した手順で、第３の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第３の情報処理装置からコンテンツおよび鍵を受信するように通信が制御され、第１の情報処理装置へのコンテンツおよび鍵の送信が制御される。

【００９８】請求項５に記載の情報処理装置、請求項６に記載の情報処理方法、および請求項７に記載のプログラム格納媒体においては、第１の情報提供装置が認証され、第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第２の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信が制御され、第２の情報提供装置または第３の情報提供装置から第１の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信が制御される。

【００９９】

【発明の実施の形態】図７は、本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。図１で説明した構成の場合と同一の部分には、図１の場合と同一の番号を付してあり、その説明は省略する。

【０１００】電話機一体型端末機５０１は、ポータブルメディア３－１が装着可能に構成され、無線により、通信ネットワーク４に接続される。電話機一体型端末機５０１は、通信ネットワーク４を介して、コンテンツサーバ２２－１または２２－２から受信したコンテンツ（所定の方式で圧縮され、暗号化されている）を、利用条件のデータ等と共にダウンロードして、コンテンツおよびその利用条件データを装着されているポータブルメディア３－１に記憶させる。

【０１０１】電話機一体型端末機５０１は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア３－１に記憶されているコンテンツを再生し、図示せぬヘッドフォンまたはスピーカなどに出力する。使用者は、電話機一体型端末機５０１を持ち歩きながら、所望の場所で所望のコンテンツをダウンロードして、そのコンテンツをポータブルメディア３－１に記憶させることができる。使用者は、電話機一体型端末機５０１に、ポータブルメディア３－１に記憶されているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【０１０２】電話機一体型端末機５０１の表示操作指示プログラム５１１は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、ダウンロードの指示などを入力して、クライアント用ＬＣＭ５１２にその指示に対応した処理を実行させる。電話機一体型端末機５０１のクライアント用ＬＣＭ５１２は、代理サーバ５０３のサーバ用ＬＣＭ５１４と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理（後述する）を実行する。

【０１０３】電話機一体型端末機５０１のクライアント用ＬＣＭ５１２は、コンテンツの不正な２次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【０１０４】クライアント用ＬＣＭ５１２は、電話機一体型端末機５０１に装着されているポータブルメディア３－１が正当であるかの認証を行い、安全な方法でサーバ５が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア３－１にコンテンツを記録させる。コンテンツの移動の処理などに伴い、クライアント用ＬＣＭ５１２は、必要な鍵を生成して、鍵を管理し、または接続されているポータブルメディア３－１との通信を制御する。

【０１０５】パーソナルコンピュータ５０２は、通信ネットワーク４に接続されている。パーソナルコンピュータ５０２は、コンテンツサーバ２２－１若しくは２２－２から受信した、またはCDから読み取ったコンテンツを、所定の圧縮の方式に変換するとともにDESなどの暗

号化方式で暗号化して記録する。パーソナルコンピュータ５０２は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

【０１０６】パーソナルコンピュータ５０２の表示操作指示プログラム１１は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、ダウンロード、またはチェックアウトの指示などを入力して、ＬＣＭ５１３にその指示に対応したダウンロード、またはチェックアウトなどの処理を実行させる。

【０１０７】パーソナルコンピュータ５０２のＬＣＭ５１３は、コンテンツの不正な２次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【０１０８】ＬＣＭ５１３は、パーソナルコンピュータ５０２に接続されたポータブルデバイス２が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、ＬＣＭ５１３は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との通信を制御する。

【０１０９】また、ＬＣＭ５１３は、ポータブルデバイス２の正当性をチェックする。ポータブルデバイス２は、ポータブルメディア３－２が装着されたとき、ポータブルメディア３－２の正当性をチェックする。ポータブルデバイス２およびポータブルメディア３－２が正当である場合、ＬＣＭ５１３は、サーバ５が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア３－２にコンテンツをチェックアウトする。ポータブルデバイス２は、パーソナルコンピュータ５０２からチェックアウトされたコンテンツを、コンテンツに関連するデータと共に、装着されているポータブルメディア３－２に記憶させる。

【０１１０】パーソナルコンピュータ５０２のＬＣＭ５１３は、暗号化して記録しているコンテンツを、接続されているポータブルデバイス２にチェックアウトする。ポータブルデバイス２は、パーソナルコンピュータ５０２からチェックアウトされたコンテンツを、コンテンツに関連するデータと共に、装着されているポータブルメディア３－２に記憶させる。

【０１１１】代理サーバ５０３を利用できるとき、パーソナルコンピュータ５０２のＰＣ用ＬＣＭ５２１（ＬＣＭ５１３の一部または全部の機能から構成される）は、代理サーバ５０３のサーバ用ＬＣＭ５１４と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理を実行する。

【０１１２】代理サーバ５０３を利用できないとき、パーソナルコンピュータ５０２のＬＣＭ５１３は、ＬＣＭ１２と同様の鍵サーバ２１－１または２１－２との認証の処理等を実行して、利用条件データおよびコンテンツ等をダウンロードする。

【０１１３】代理サーバ５０３は、サーバ用ＬＣＭ５１４を実行して、相互認証した電話機一体型端末機５０１または相互認証したパーソナルコンピュータ５０２の要求に対応して、鍵サーバ２１－１または２１－２との認証の処理を実行する。代理サーバ５０３は、鍵サーバ２１－１または２１－２との相互認証の処理の後、鍵サーバ２１－１または２１－２からコンテンツ鍵を受信して、受信したコンテンツ鍵を電話機一体型端末機５０１またはパーソナルコンピュータ５０２に供給する。代理サーバ５０３は、コンテンツサーバ２２－１または２２－２からコンテンツを受信して、受信したコンテンツを電話機一体型端末機５０１またはパーソナルコンピュータ５０２に供給する。

【０１１４】代理サーバ５０３は、サーバ５－１からコンテンツおよびコンテンツ鍵をダウンロードするとき、サーバ５－１からコンテンツを受信した後、コンテンツ鍵を受信する。代理サーバ５０３は、サーバ５－２からコンテンツおよびコンテンツ鍵をダウンロードするとき、コンテンツ鍵を受信した後、コンテンツを受信する。

【０１１５】代理サーバ５０３は、サーバ５－１からコンテンツおよびコンテンツ鍵をダウンロードしたときも、サーバ５－２からコンテンツおよびコンテンツ鍵をダウンロードしたときも、いずれの場合も、同一の手順（例えば、コンテンツ鍵を送信してから、コンテンツを送信する）で、電話機一体型端末機５０１またはパーソナルコンピュータ５０２にコンテンツおよびコンテンツ鍵を供給する。

【０１１６】電話機一体型端末機５０１またはパーソナルコンピュータ５０２は、代理サーバ５０３を介して、サーバ５－１または５－２からコンテンツおよびコンテンツ鍵をダウンロードすることにより、同一の手順でコンテンツおよびコンテンツ鍵を受信することができる。

【０１１７】図８は、電話機一体型端末機５０１の構成を説明する図である。CPU（CentralProcessing Unit）６０１は、ROM（Read-only Memory）６０２またはRAM（Random-Access Memory）６０３に格納されている各種プログラムを実際に実行する。ROM６０２は、EEPROM（Electrically Erasable Programmable Read-Only Memory）またはフラッシュメモリなどで構成され、一般的には、CPU６０１が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM６０３は、SRAM（Static RAM）などで構成され、CPU６０１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。

【０１１８】入力部６０５は、入力キーまたはマイクロフォンなどで構成され、CPU６０１に各種の指令を入力するとき、または音声などを入力するとき、使用者により操作される。表示部６０６は、液晶表示装置などから成り、各種情報をテキストやイメージで表示する。

【０１１９】音声再生部６０７は、通信部６０８から供給された通話相手の音声のデータ、またはインターフェース６０９から供給されたポータブルメディア３－１に記憶されているコンテンツを再生して、音声を出力する。

【０１２０】通信部６０８は、公衆回線網３１と接続し、CPU６０１から供給されたデータ（例えば、コンテンツの送信要求など）または入力部６０５から供給された使用者の音声のデータを、所定の方式のパケットに格納して、公衆回線網３１を介して、送信する。また、通信部６０８は、公衆回線網３１を介して、受信したパケットに格納されているデータ（例えば、コンテンツなど）または通話相手の音声のデータをCPU６０１、RAM６０３、音声再生部６０７、またはインターフェース６０９に出力する。

【０１２１】インターフェース６０９は、CPU６０１、RAM６０３、または通信部６０８から供給されたデータを装着されているポータブルメディア３－１に記憶させるとともに、装着されているポータブルメディア３－１からコンテンツなどのデータを読み出して、CPU６０１、RAM６０３、または音声再生部６０７に供給する。

【０１２２】インターフェース６１０は、外付けのドライブ６３１が接続される。ドライブ６３１は、装着されている磁気ディスク６４１、光ディスク６４２（CD-ROMを含む）、光磁気ディスク６４３、または半導体メモリ６４４に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース６１０、およびバス６０４を介して接続されているROM６０２またはRAM６０３に供給する。

【０１２３】CPU６０１乃至インターフェース６１０は、バス６０４により相互に接続されている。

【０１２４】図９は、代理サーバ５０３の構成を説明する図である。CPU６５１は、各種アプリケーションプログラム（詳細については後述する）や、OS（Operating System)を実際に実行する。ROM６５２は、一般的には、CPU６５１が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM６５３は、CPU６５１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス６５４により相互に接続されている。

【０１２５】ホストバス６５４は、ブリッジ６５５を介して、PCI(Peripheral Component Interconnect/Interface)バスなどの外部バス６５６に接続されている。

【０１２６】キーボード６５８は、CPU６５１に各種の指令を入力するとき、使用者により操作される。ポインティングデバイス６５９は、ディスプレイ６６０の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ６６０は、液晶表示装置またはCRT（Cathode Ray Tube）などから成り、各種情報をテキストやイメージで表示する。HDD（Hard Disk Drive）６６１は、ハードディスクを駆動し、それらにCPU６５１によって実行するプログラムや情報を記録または再生させる。

【０１２７】ドライブ６６２は、装着されている磁気ディスク６８１、光ディスク６８２、光磁気ディスク６８３、または半導体メモリ６８４に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース６５７、外部バス６５６、ブリッジ６５５、およびホストバス６５４を介して接続されているRAM６５３に供給する。

【０１２８】これらのキーボード６５８乃至ドライブ６６２は、インターフェース６５７に接続されており、インターフェース６５７は、外部バス６５６、ブリッジ６５５、およびホストバス６５４を介してCPU６５１に接続されている。

【０１２９】通信部６６３は、通信ネットワーク４が接続され、CPU６５１、またはHDD６６１から供給されたデータ（例えば、コンテンツ鍵など）を、所定の方式のパケットに格納して、通信ネットワーク４を介して、送信するとともに、通信ネットワーク４を介して、受信したパケットに格納されているデータ（例えば、コンテンツＩＤなど）をCPU６５１、RAM６５３、またはHDD６６１に出力する。

【０１３０】通信部６６３は、外部バス６５６、ブリッジ６５５、およびホストバス６５４を介してCPU６５１に接続されている。

【０１３１】次に、図１０を参照して、本願のデジタルデータ伝送システムの機能の構成について説明する。図２で説明した構成の場合と同一の部分には、図２の場合と同一の番号を付してあり、その説明は省略する。

【０１３２】電話機一体型端末機５０１は、表示操作指示プログラム５１１、クライアント用ＬＣＭ５１２、ＩＰ通信プログラム７０１、ＩＳＰ接続プログラム７０２、およびＰＨＳ／ＩＭＴ通信プログラム７０３を実行する。

【０１３３】ＰＨＳ／ＩＭＴ通信プログラム７０３は、公衆回線網３１を介して通信を行うためのプログラムである。ＩＳＰ接続プログラム７０２は、ＩＳＰ３２と接続するためのプログラムである。ＩＰ通信プログラム７０１は、ＨＴＴＰ７４１およびＷａｐ７４２などの手続を包含し、通信ネットワーク４を介して、鍵サーバ２１－１、コンテンツサーバ２２－１、ショップサーバ２３－１、鍵サーバ２１－２、コンテンツサーバ２２－２、ショップサーバ２３－２、または代理サーバ５０３など

と通信するためのプログラムである。
【０１３４】クライアント用ＬＣＭ５１２は、ライセンス管理プログラム７１１、ダウンロードプログラム７１２、およびフォーマット管理プログラム７１３などから構成されている。
【０１３５】ライセンス管理プログラム７１１は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム７２１、サーバ認証プログラム７２２、およびPM認証プログラム７２３などから構成されている。
【０１３６】利用条件管理プログラム７２１は、コンテンツの利用条件に基づいて、ポータブルメディア３－１が記憶しているコンテンツの再生などを許可するか、または禁止するかなどの管理を実行するとともに、ポータブルメディア３－１が記憶しているコンテンツの再生などに対応して、ポータブルメディア３－１に、ポータブルメディア３－１が記憶している利用条件のデータを更新させる。サーバ認証プログラム７２２は、通信ネットワーク４を介して、代理サーバ５０３を認証する。PM認証プログラム７２３は、ポータブルメディア３－１が電話機一体型端末機５０１に装着されたとき、ポータブルメディア３－１を認証する。
【０１３７】ダウンロードプログラム７１２は、鍵管理プログラム７２４、コンテンツ管理プログラム７２５、鍵情報受信プログラム７２６、およびコンテンツ情報受信プログラム７２７などから構成されている。
【０１３８】鍵管理プログラム７２４は、代理サーバ５０３からコンテンツ鍵を受信して、コンテンツに対応させて、コンテンツ鍵をポータブルメディア３－１に記憶させて、管理する。鍵管理プログラム７２４は、代理サーバ５０３からコンテンツ鍵を受信する受信プログラム７３１などを含む。
【０１３９】コンテンツ管理プログラム７２５は、代理サーバ５０３からコンテンツの利用条件とともにコンテンツ（暗号化されている）を受信して、コンテンツの利用条件とともにコンテンツをポータブルメディア３－１に記憶させる。コンテンツ管理プログラム７２５の受信プログラム７３２は、代理サーバ５０３からコンテンツの利用条件およびコンテンツを受信する。
【０１４０】鍵情報受信プログラム７２６は、ショップサーバ２３－１または２３－２から、コンテンツに対応するコンテンツ鍵を供給する鍵サーバ２１－１または２１－２を特定するＵＲＬを受信する。コンテンツ情報受信プログラム７２７は、ショップサーバ２３－１または２３－２から、所望のコンテンツを特定するコンテンツＩＤ、および所望のコンテンツを供給するコンテンツサーバ２２－１または２２－２を特定するＵＲＬを受信する。
【０１４１】フォーマット管理プログラム７１３は、代理サーバ５０３を介して、コンテンツサーバ２２－１または２２－２からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換する。フォーマット管理プログラム７１３は、システム識別プログラム７２８およびフォーマット変換プログラム７２９などから構成されている。
【０１４２】システム識別プログラム７２８は、コンテンツのダウンロード先が、サーバ５－１であるか、サーバ５－２であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム７２９は、コンテンツの符号化方式および暗号化方式を変換する。
【０１４３】次に、代理サーバ５０３の構成について説明する。代理サーバ５０３は、サーバ用ＬＣＭ５１４、およびＩＰ通信プログラム７５１を実行する。
【０１４４】サーバ用ＬＣＭ５１４は、ライセンス管理プログラム７６１、およびシーケンス管理プログラム７６２などを含む。
【０１４５】ライセンス管理プログラム７６１は、更に、鍵サーバ２１－１または２１－２を認証するサーバ認証プログラム７８１、および電話機一体型端末機５０１を認証するＰＤ認証プログラム７８２などを含む。
【０１４６】シーケンス管理プログラム７６２は、鍵管理プログラム７７１、コンテンツ管理プログラム７７２、およびシステム識別プログラム７７３などを含む。
【０１４７】鍵管理プログラム７７１は、更に、通信ネットワーク４を介して、鍵サーバ２１－１または２１－２からコンテンツ鍵を受信する鍵受信プログラム７８３、および通信ネットワーク４を介して、受信したコンテンツ鍵を電話機一体型端末機５０１に配信する鍵配信プログラム７８４などを含む。
【０１４８】コンテンツ管理プログラム７７２は、更に、通信ネットワーク４を介して、コンテンツサーバ２２－１または２２－２からコンテンツを受信するコンテンツ受信プログラム７８５、および通信ネットワーク４を介して、受信したコンテンツを電話機一体型端末機５０１に配信するコンテンツ配信プログラム７８６などを含む。
【０１４９】システム識別プログラム７７３は、電話機一体型端末機５０１から供給されたコンテンツＩＤを基に、コンテンツのダウンロード先が、サーバ５－１であるか、サーバ５－２であるかのいずれかを識別するためのプログラムである。
【０１５０】ＩＰ通信プログラム７５１は、ＨＴＴＰ７８７およびＷａｐ７８８などの手続を包含し、通信ネットワーク４を介して、サーバ５－１若しくは５－２、または電話機一体型端末機５０１と通信するためのプログラムである。
【０１５１】次に、電話機一体型端末機５０１がサーバ５－１からコンテンツをダウンロードする処理を図１１および図１２のフローチャートを参照して説明する。ステップＳ２１０１において、電話機一体型端末機５０１

のＰＨＳ／ＩＭＴ通信プログラム７０３は、公衆回線網３１と接続を確立する。ステップＳ２２０１において、公衆回線網３１の図示せぬ地上局などは、電話機一体型端末機５０１と接続を確立する。

【０１５２】ステップＳ２１０２において、電話機一体型端末機５０１のＩＳＰ接続プログラム７０２は、電話機一体型端末機５０１と公衆回線網３１との接続を介して、ＩＳＰ３２と接続を確立する。ステップＳ２３０１において、ＩＳＰ３２は、電話機一体型端末機５０１と公衆回線網３１との接続を介して、電話機一体型端末機５０１と接続を確立する。

【０１５３】以降の電話機一体型端末機５０１と、鍵サーバ２１－１、コンテンツサーバ２２－１、ショップサーバ２３－１、または代理サーバ５０３との処理は、電話機一体型端末機５０１とＩＳＰ３２との接続を介して実行される。

【０１５４】ステップＳ２１０３において、電話機一体型端末機５０１のＩＰ通信プログラム７０１は、ショップサーバ２３－１とＩＰ通信を確立する。ステップＳ２４０１において、ショップサーバ２３－１のＩＰ通信プログラム１２４は、電話機一体型端末機５０１とＩＰ通信を確立する。

【０１５５】ステップＳ２４０２において、ショップサーバ２３－１の閲覧プログラム１２３は、通信ネットワーク４を介して、電話機一体型端末機５０１に閲覧用（コンテンツの選択用）のデジタルデータを送信する。ステップＳ２１０４において、電話機一体型端末機５０１の図示せぬブラウザプログラムは、受信したデジタルデータに対応するテキストまたは画像を表示部６０６に表示させ、使用者に閲覧させる。また、電話機一体型端末機５０１のブラウザプログラムは、コンテンツのストリーミング再生により、コンテンツを音声再生部６０７に再生させて、使用者に試聴させたり、または、キーワードにより所望のコンテンツをショップサーバ２３－１の閲覧プログラム１２３に検索させ、その結果を表示部６０６に表示させる。

【０１５６】ステップＳ２４０２およびステップＳ２１０４の処理は、電話機一体型端末機５０１の使用者の要求に対応して、例えば、使用者が購入するコンテンツを決定するまで繰り返される。

【０１５７】ステップＳ２１０５において、電話機一体型端末機５０１のブラウザプログラムは、通信ネットワーク４を介して、購入依頼をショップサーバ２３－１に送信する。ステップＳ２４０３において、ショップサーバ２３－１の閲覧プログラム１２３は、電話機一体型端末機５０１から送信された購入依頼を受信する。

【０１５８】ステップＳ２４０４において、ショップサーバ２３－１のコンテンツ情報送信プログラム１２２は、ステップＳ２４０３の処理で受信した購入依頼に対応して、コンテンツを配信するコンテンツサーバ２２－１のＵＲＬ、およびコンテンツを特定するためのコンテンツＩＤなどを含む、コンテンツ情報を、通信ネットワーク４を介して、電話機一体型端末機５０１に送信する。ステップＳ２１０６において、電話機一体型端末機５０１のコンテンツ情報受信プログラム７２７は、ショップサーバ２３－１が送信した、コンテンツ情報を受信する。

【０１５９】ステップＳ２４０５において、ショップサーバ２３－１の鍵情報送信プログラム１２１は、ステップＳ２４０３の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ２１－１のＵＲＬなどの、鍵情報を通信ネットワーク４を介して、電話機一体型端末機５０１に送信する。ステップＳ２１０７において、電話機一体型端末機５０１の鍵情報受信プログラム７２６は、ショップサーバ２３－１が送信した、鍵情報を受信する。

【０１６０】ステップＳ２１０８において、電話機一体型端末機５０１のＩＰ通信プログラム７０１は、予め記録している代理サーバ５０３のＵＲＬを基に、代理サーバ５０３とＩＰ通信を確立する。ステップＳ２５０１において、代理サーバ５０３のＩＰ通信プログラム７５１は、電話機一体型端末機５０１とＩＰ通信を確立する。

【０１６１】ステップＳ２１０９において、電話機一体型端末機５０１のライセンス管理プログラム７１１のサーバ認証プログラム７２２は、代理サーバ５０３を認証する。ステップＳ２５０２において、代理サーバ５０３のライセンス管理プログラム７６１のPD認証プログラム７８２は、電話機一体型端末機５０１を認証する。

【０１６２】ステップＳ２１０９およびステップＳ２５０２における電話機一体型端末機５０１と代理サーバ５０３との相互認証の処理は、チャレンジレスポンス方式の認証の処理であり、ステップＳ１１２およびステップＳ６０２における鍵サーバ２１－１とパーソナルコンピュータ１との相互認証の処理に比較して、演算量が少なく、少ない演算能力、または記憶容量でも、迅速に実行することができる。電話機一体型端末機５０１および代理サーバ５０３は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

【０１６３】ステップＳ２１０９およびステップＳ２５０２における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、電話機一体型端末機５０１がコンテンツをダウンロードする処理は、コンテンツをダウンロードしないで、終了する。

【０１６４】ステップＳ２１１０において、電話機一体型端末機５０１のコンテンツ管理プログラム７２５は、コンテンツＩＤを代理サーバ５０３に送信する。ステップＳ２５０３において、代理サーバ５０３は、電話機一体型端末機５０１が送信したコンテンツＩＤを受信する。ステップＳ２１１１において、電話機一体型端末機５０１の鍵管理プログラム７２４は、ステップＳ２１０

７の処理で受信した鍵情報を代理サーバ５０３に送信する。ステップＳ２５０４において、代理サーバ５０３は、電話機一体型端末機５０１が送信した、鍵情報を受信する。

【０１６５】ステップＳ２５０５において、代理サーバ５０３のシステム識別プログラム７７３は、ステップＳ２５０３の処理で受信したコンテンツＩＤを基に、コンテンツおよびコンテンツ鍵のダウンロード先が、サーバ５－１であることを識別する。

【０１６６】なお、ステップＳ２１１０において、電話機一体型端末機５０１は、コンテンツＩＤと共にコンテンツサーバ２２－１のＵＲＬを送信して、ステップＳ２５０３において、代理サーバ５０３は、コンテンツＩＤと共にコンテンツサーバ２２－１のＵＲＬを受信するようにしてもよい。

【０１６７】ステップＳ２５０６において、代理サーバ５０３のＩＰ通信プログラム７５１は、ステップＳ２５０５の処理の識別の結果を基に、コンテンツサーバ２２－１とＩＰ通信を確立する。ステップＳ２６０１において、コンテンツサーバ２２－１のＩＰ通信プログラム１９３は、代理サーバ５０３とＩＰ通信を確立する。

【０１６８】ステップＳ２５０７において、代理サーバ５０３のコンテンツ管理プログラム７７２は、ステップＳ２５０３の処理で取得したコンテンツＩＤを、通信ネットワーク４を介して、コンテンツサーバ２２－１に送信する。ステップＳ２６０２において、コンテンツサーバ２２－１は、代理サーバ５０３が送信したコンテンツＩＤを受信する。ステップＳ２６０３において、コンテンツサーバ２２－１のコンテンツ配信プログラム１９２は、ステップＳ２６０２で受信したコンテンツＩＤに対応するコンテンツ（暗号化されている）を、コンテンツ保存プログラム１９１から読み出して、通信ネットワーク４を介して、代理サーバ５０３に配信する。

【０１６９】ステップＳ２５０８において、代理サーバ５０３のコンテンツ管理プログラム７７２の受信プログラム７８５は、コンテンツサーバ２２－１が送信したコンテンツを受信する。

【０１７０】ステップＳ２５０９において、代理サーバ５０３のＩＰ通信プログラム７５１は、ステップＳ２５０５の処理の識別の結果を基に、鍵サーバ２１－１とＩＰ通信を確立する。ステップＳ２７０１において、鍵サーバ２１－１のＩＰ通信プログラム１５５は、代理サーバ５０３とＩＰ通信を確立する。

【０１７１】ステップＳ２５１０において、代理サーバ５０３のライセンス管理プログラム７６１のサーバ認証プログラム７８１は、鍵サーバ２１－１を認証する。ステップＳ２７０２において、鍵サーバ２１－１の認証プログラム１５１は、代理サーバ５０３を認証する。

【０１７２】例えば、鍵サーバ２１－１には、マスター鍵ＫMSSが予め記憶されており、代理サーバ５０３には、個別鍵ＫPCCと代理サーバ５０３のIDが予め記憶されている。代理サーバ５０３には、更に、マスター鍵ＫMCCが予め記憶されており、鍵サーバ２１－１にも鍵サーバ２１－１のIDと個別鍵ＫPSSが記憶されている。

【０１７３】鍵サーバ２１－１は、代理サーバ５０３から、代理サーバ５０３のIDの供給を受け、そのIDと自分自身が有するマスター鍵ＫMSSにハッシュ関数を適用して、代理サーバ５０３の個別鍵ＫPCCと同一の鍵を生成する。

【０１７４】代理サーバ５０３は、鍵サーバ２１－１から、鍵サーバ２１－１のIDの供給を受け、そのIDと自分自身が有するマスター鍵ＫMCCにハッシュ関数を適用して、鍵サーバ２１－１の個別鍵ＫPSSと同一の鍵を生成する。このようにすることで、代理サーバ５０３と鍵サーバ２１－１の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時的な一時鍵を生成する。

【０１７５】ステップＳ２５１０またはステップＳ２７０２における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、処理は終了する。

【０１７６】ステップＳ２５１１において、代理サーバ５０３の鍵管理プログラム７７１は、ステップＳ２５０３の処理で取得したコンテンツＩＤを鍵サーバ２１－１に送信する。ステップＳ２７０３において、鍵サーバ２１－１は、代理サーバ５０３が送信したコンテンツＩＤを受信する。ステップＳ２７０４において、鍵サーバ２１－１の鍵配信プログラム１５２は、鍵保存プログラム１５３がコンテンツＩＤと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク４を介して、そのコンテンツ鍵（鍵サーバ２１－１と代理サーバ５０３とで共有する一時鍵で暗号化されている）を代理サーバ５０３に送信する。ステップＳ２５１２において、代理サーバ５０３の鍵管理プログラム７７１の鍵受信プログラム７８３は、鍵サーバ２１－１が送信したコンテンツ鍵を受信する。

【０１７７】ステップＳ２５１３において、代理サーバ５０３の鍵管理プログラム７７１の鍵配信プログラム７８４は、ステップＳ２５１２の処理で受信したコンテンツ鍵を、鍵サーバ２１－１と代理サーバ５０３とで共有する一時鍵で復号し、電話機一体型端末機５０１と代理サーバ５０３で共有する一時鍵で暗号化して、通信ネットワーク４を介して、暗号化されているコンテンツ鍵を電話機一体型端末機５０１に送信する。ステップＳ２１１２において、電話機一体型端末機５０１の鍵管理プログラム７２４の受信プログラム７３１は、代理サーバ５０３が送信したコンテンツ鍵を受信する。鍵管理プログラム７２４は、コンテンツ鍵を電話機一体型端末機５０１と代理サーバ５０３で共有する一時鍵で復号して、ポータブルメディア３－１の鍵管理プログラム１０２に供給し、鍵管理プログラム１０２に、コンテンツ鍵を記憶

させる。
【０１７８】ステップＳ２５１４において、代理サーバ５０３のコンテンツ管理プログラム７７２のコンテンツ配信プログラム７８６は、通信ネットワーク４を介して、暗号化されているコンテンツを電話機一体型端末機５０１に送信する。ステップＳ２１１３において、電話機一体型端末機５０１のコンテンツ管理プログラム７２５の受信プログラム７３２は、代理サーバ５０３が送信したコンテンツを受信する。
【０１７９】ステップＳ２１１４において、電話機一体型端末機５０１のＰＨＳ／ＩＭＴ通信プログラム７０３は、公衆回線網３１との接続を切断する。ステップＳ２２０２において、公衆回線網３１の図示せぬ地上局などは、電話機一体型端末機５０１と接続を切断する。
【０１８０】ステップＳ２１１５において、電話機一体型端末機５０１のフォーマット管理プログラム７１３は、ステップＳ２１１３の処理で受信したコンテンツのフォーマットを変換する。コンテンツ管理プログラム７２５は、フォーマットを変換したコンテンツを、インターフェース６０９を介して、ポータブルメディア３－１に供給して、コンテンツ管理プログラム１０３に、コンテンツを記憶させ、処理は終了する。
【０１８１】次に、電話機一体型端末機５０１がサーバ５－２からコンテンツをダウンロードする処理を図１３および図１４のフローチャートを参照して説明する。ステップＳ３１０１乃至ステップＳ３５０４の処理は、サーバ５－２、並びにＩＰ通信プログラム７０１、ＩＳＰ接続プログラム７０２、ＰＨＳ／ＩＭＴ通信プログラム７０３、およびダウンロードプログラム７１２により実行され、それぞれ、ステップＳ２１０１乃至ステップＳ２５０４の処理と同様なので、その説明は省略する。
【０１８２】ステップＳ３５０５において、代理サーバ５０３のシステム識別プログラム７７３は、ステップＳ３５０３の処理で受信したコンテンツＩＤを基に、コンテンツおよびコンテンツ鍵のダウンロード先が、サーバ５－２であることを識別する。
【０１８３】ステップＳ３５０６において、代理サーバ５０３のＩＰ通信プログラム７５１は、ステップＳ３５０５の識別の処理の結果を基に、鍵サーバ２１－２とＩＰ通信を確立する。ステップＳ３７０１において、鍵サーバ２１－２は、代理サーバ５０３とＩＰ通信を確立する。
【０１８４】ステップＳ３５０７において、代理サーバ５０３のサーバ認証プログラム７８１は、鍵サーバ２１－２を認証する。ステップＳ３７０２において、鍵サーバ２１－２は、代理サーバ５０３を認証する。
【０１８５】ステップＳ３５０７およびステップＳ３７０２の処理は、ステップＳ２５１０およびステップＳ２７０２の処理と同様の処理である。
【０１８６】ステップＳ３５０７またはステップＳ３７０２における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、処理は終了する。
【０１８７】ステップＳ３５０８において、代理サーバ５０３の鍵管理プログラム７７１は、ステップＳ３５０３の処理で取得したコンテンツＩＤを鍵サーバ２１－２に送信する。ステップＳ３７０３において、鍵サーバ２１－２は、代理サーバ５０３が送信したコンテンツＩＤを受信する。ステップＳ３７０４において、鍵サーバ２１－２は、コンテンツＩＤと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク４を介して、そのコンテンツ鍵（鍵サーバ２１－２と代理サーバ５０３とで共有する一時鍵で暗号化されている）を代理サーバ５０３に送信する。ステップＳ３５０９において、代理サーバ５０３の鍵管理プログラム７７１の鍵受信プログラム７８３は、鍵サーバ２１－２が送信したコンテンツ鍵を受信する。
【０１８８】ステップＳ３５１０において、代理サーバ５０３のＩＰ通信プログラム７５１は、ステップＳ３５０５の識別の処理の結果を基に、コンテンツサーバ２２－２とＩＰ通信を確立する。ステップＳ３６０１において、コンテンツサーバ２２－２は、代理サーバ５０３とＩＰ通信を確立する。
【０１８９】ステップＳ３５１１において、代理サーバ５０３のコンテンツ管理プログラム７７２は、ステップＳ３５０３の処理で取得したコンテンツＩＤを、通信ネットワーク４を介して、コンテンツサーバ２２－２に送信する。ステップＳ３６０２において、コンテンツサーバ２２－２は、代理サーバ５０３が送信したコンテンツＩＤを受信する。ステップＳ３６０３において、コンテンツサーバ２２－２は、ステップＳ３６０２で受信したコンテンツＩＤに対応するコンテンツ（暗号化されている）を読み出して、通信ネットワーク４を介して、代理サーバ５０３に配信する。
【０１９０】ステップＳ３５１２において、代理サーバ５０３のコンテンツ管理プログラム７７２の受信プログラム７８５は、コンテンツサーバ２２－２が送信したコンテンツを受信する。
【０１９１】ステップＳ３５１２乃至ステップＳ３１１５の処理は、ステップＳ２５１３乃至ステップＳ２１１５の処理と同様なので、その説明は省略する。
【０１９２】以上のように、電話機一体型端末機５０１は、代理サーバ５０３を介することにより、サーバ５－１からコンテンツおよびコンテンツ鍵をダウンロードするときも、サーバ５－２からコンテンツおよびコンテンツ鍵をダウンロードするときも、いずれの場合も、同一の手順（例えば、コンテンツ鍵を受信してから、コンテンツを受信する）で、コンテンツおよびコンテンツ鍵を受信することができる。
【０１９３】また、図１１乃至図１４のフローチャートを参照して説明した手順は、後述する代理サーバ５０３

がコンテンツの符号化方式および暗号化方式を変換する処理（図１６および図１７のフローチャートを参照して説明する）に比較して、電話機一体型端末機５０１が公衆回線網３１に接続している時間を短くすることができる。

【０１９４】次に、図１５を参照して、本願のデジタルデータ伝送システムの他の機能の構成について説明する。図１０で説明した構成の場合と同一の部分には、図１０の場合と同一の番号を付してあり、その説明は省略する。

【０１９５】図１５に示す電話機一体型端末機５０１は、フォーマット管理プログラム７１３を有しない。

【０１９６】図１５に示す代理サーバ５０３のサーバ用ＬＣＭ５１４は、ライセンス管理プログラム７６１およびシーケンス管理プログラム７６２に加えて、フォーマット管理プログラム８０１を含む。

【０１９７】フォーマット管理プログラム８０１は、コンテンツサーバ２２－１または２２－２からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換する。フォーマット管理プログラム８０１は、システム識別プログラム８１１およびフォーマット変換プログラム８１２から構成されている。

【０１９８】システム識別プログラム８１１は、コンテンツのダウンロード先が、サーバ５－１であるか、サーバ５－２であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム８１２は、コンテンツの符号化方式および暗号化方式を変換する。

【０１９９】次に、図１５にその構成を示す電話機一体型端末機５０１および代理サーバ５０３がサーバ５－２からコンテンツをダウンロードする処理を図１６および図１７のフローチャートを参照して説明する。

【０２００】ステップＳ４１０１乃至ステップＳ４５１２の処理は、それぞれ、ステップＳ３１０１乃至ステップＳ３５１２の処理と同様なので、その説明は省略する。

【０２０１】ステップＳ４５１２において、代理サーバ５０３のフォーマット管理プログラム８０１は、ステップＳ４５１２の処理で受信したコンテンツのフォーマットを変換する。

【０２０２】ステップＳ４５１４において、代理サーバ５０３の鍵管理プログラム７７１の鍵配信プログラム７８４は、ステップＳ４５０９の処理で受信したコンテンツ鍵を、鍵サーバ２１－２と代理サーバ５０３とで共有する一時鍵で復号し、電話機一体型端末機５０１と代理サーバ５０３で共有する一時鍵で暗号化して、通信ネットワーク４を介して、暗号化されているコンテンツ鍵を電話機一体型端末機５０１に送信する。ステップＳ４１１２において、電話機一体型端末機５０１の鍵管理プログラム７２４の受信プログラム７３１は、代理サーバ５０３が送信したコンテンツ鍵を受信する。鍵管理プログラム７２４は、コンテンツ鍵を電話機一体型端末機５０１と代理サーバ５０３で共有する一時鍵で復号して、ポータブルメディア３－１の鍵管理プログラム１０２に供給し、鍵管理プログラム１０２に、コンテンツ鍵を記憶させる。

【０２０３】ステップＳ４５１５において、代理サーバ５０３のコンテンツ管理プログラム７７２のコンテンツ配信プログラム７８６は、通信ネットワーク４を介して、暗号化されているコンテンツを電話機一体型端末機５０１に送信する。ステップＳ４１１３において、電話機一体型端末機５０１のコンテンツ管理プログラム７２５の受信プログラム７３２は、代理サーバ５０３が送信したコンテンツを受信する。コンテンツ管理プログラム７２５は、受信したコンテンツ（フォーマットが変換されている）を、インターフェース６０９を介して、ポータブルメディア３－１に供給して、コンテンツ管理プログラム１０３に、コンテンツを記憶させる。

【０２０４】ステップＳ４１１４において、電話機一体型端末機５０１のＰＨＳ／ＩＭＴ通信プログラム７０３は、公衆回線網３１との接続を切断する。ステップＳ４２０２において、公衆回線網３１の図示せぬ地上局などは、電話機一体型端末機５０１と接続を切断して、処理は終了する。

【０２０５】なお、サーバ５－１からコンテンツおよびコンテンツ鍵を受信する処理は、代理サーバ５０３がサーバ５－１よりコンテンツを受信した後、サーバ５－１よりコンテンツ鍵を受信する手順となり、同様に行われる。

【０２０６】このように、代理サーバ５０３は、サーバ５－１または５－２から受信したコンテンツの符号化方式および暗号化方式を変換して、電話機一体型端末機５０１に供給することもできる。この場合、電話機一体型端末機５０１は、コンテンツの符号化方式および暗号化方式を変換するプログラムが不要となる。従って、電話機一体型端末機５０１は、図１０に示す場合に比較して、より少ない演算能力または記憶容量でも、迅速にコンテンツを受信する処理を実行することができる。

【０２０７】また、コンテンツは、楽音のデータであると説明したが、楽音のデータに限らず、静止画像のデータ、動画像のデータ、テキストのデータ、またはプログラムなどでもよい。

【０２０８】なお、電話機一体型端末機５０１またはパーソナルコンピュータ５０２が、コンテンツをダウンロードすると説明したが、電話機一体型端末機５０１またはパーソナルコンピュータ５０２に限らず、携帯電話機、ＰＤＡ（Personal DigitalAssistant）、通信機能付き撮像機能付きデジタルビデオカセットレコーダ、通信機能付き電子手帳装置、または携帯型パーソナルコンピュータなどがコンテンツをダウンロードするようにしてもよい。

【０２０９】また、電話機一体型端末機５０１は、ＰＨＳまたはＩＭＴにより通信すると説明したが、ＰＨＳまたはＩＭＴに限らず、W-CDMA（Code Division Multiple Access）、衛星通信、衛星放送、PSTN（Public Switched telephone network）、xDSL（x Digital Subscriber Line）、ISDN（Integrated Services Digital Network）、またはプライベートネットワークなどで通信するようにしてもよい。

【０２１０】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【０２１１】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図８または図９に示すように、磁気ディスク６４１若しくは磁気ディスク６８１（いずれもフロッピディスクを含む）、光ディスク６４２若しくは光ディスク６８２（いずれも、CD-ROM(Compact Disc-Read Only Memory)、ＤＶＤ(Digital Versatile Disc)を含む）、光磁気ディスク６４３若しくは光磁気ディスク６８３（いずれもＭＤ(Mini-Disc)を含む）、若しくは半導体メモリ６４４若しくは半導体メモリ６８４などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM６０２若しくはROM６５２や、HDD６６１などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部６０８または通信部６６３を介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【０２１２】なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２１３】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０２１４】

【発明の効果】請求項１に記載の情報提供装置、請求項３に記載の情報提供方法、および請求項４に記載のプログラム格納媒体によれば、第ｉの情報処理装置が認証され、第２の情報処理装置または第３の情報処理装置が認証され、第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第２の情報処理装置を特定するデータまたは第３の情報処理装置を特定するデータの受信が制御され、第２の情報処理装置を特定するデータを受信した場合、第２の情報処理装置に対応した手順で、第２の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第２の情報処理装置からコンテンツおよび鍵を受信し、第３の情報処理装置を特定するデータを受信した場合、第３の情報処理装置に対応した手順で、第３の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第３の情報処理装置からコンテンツおよび鍵を受信するように通信が制御され、第１の情報処理装置へのコンテンツおよび鍵の送信が制御されるようにしたので、第１の情報処理装置の処理能力が小さくとも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようになる。

【０２１５】請求項５に記載の情報処理装置、請求項６に記載の情報処理方法、および請求項７に記載のプログラム格納媒体によれば、第１の情報提供装置が認証され、第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第２の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信が制御され、第２の情報提供装置または第３の情報提供装置から第１の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信が制御されるようにしたので、処理能力が小さくとも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようになる。

【図面の簡単な説明】

【図１】従来のデジタルデータ伝送システムの構成を示す図である。

【図２】従来のデジタルデータ伝送システムの機能の構成を示す図である。

【図３】パーソナルコンピュータ１がサーバ５－１からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする従来の処理を説明するフローチャートである。

【図４】パーソナルコンピュータ１がサーバ５－１からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする従来の処理を説明するフローチャートである。

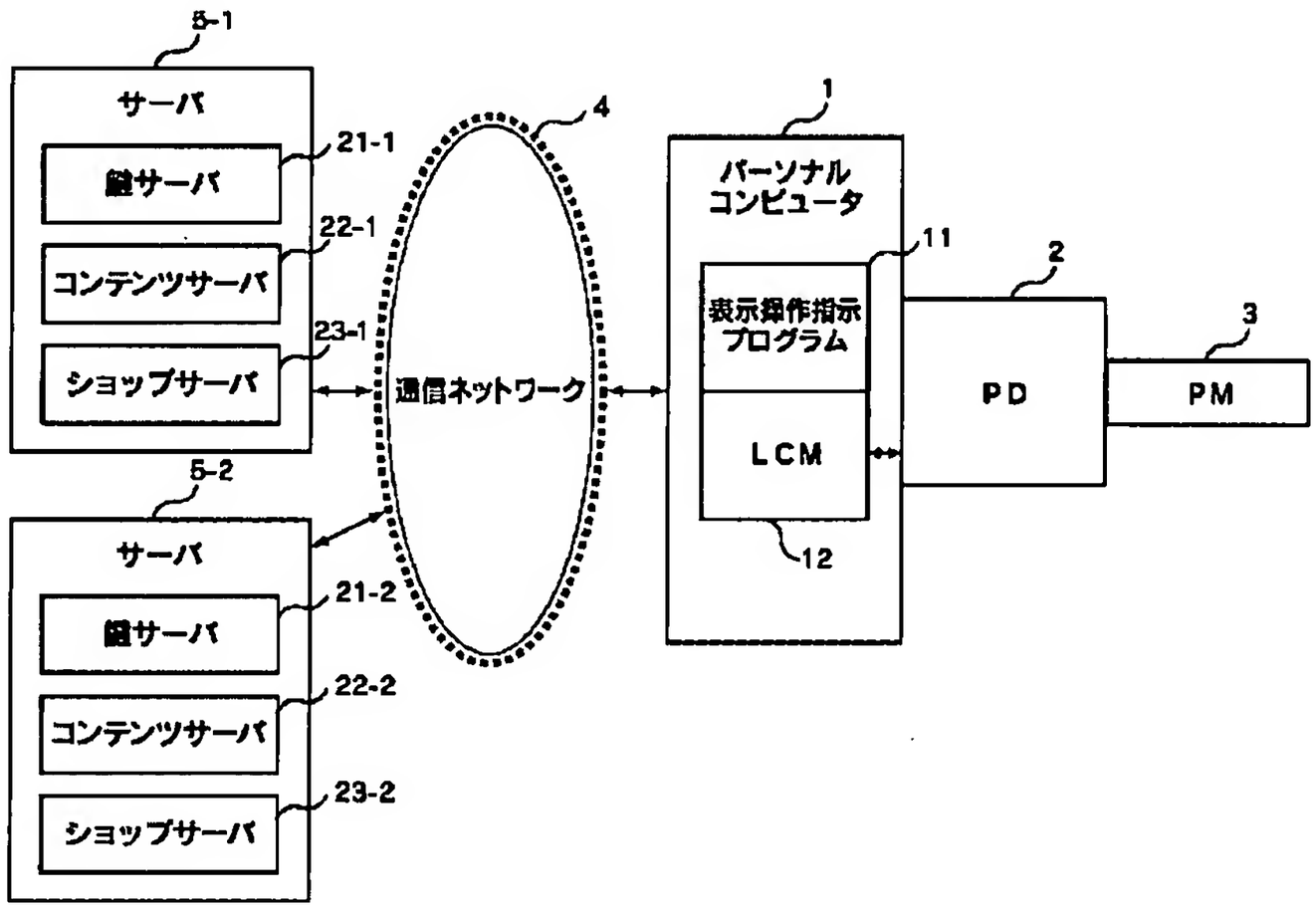
【図５】パーソナルコンピュータ１がサーバ５－２からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする従来の処理を説明するフローチャートである。

【図６】パーソナルコンピュータ１がサーバ５－２からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする従来の処理を説明するフローチャートである。

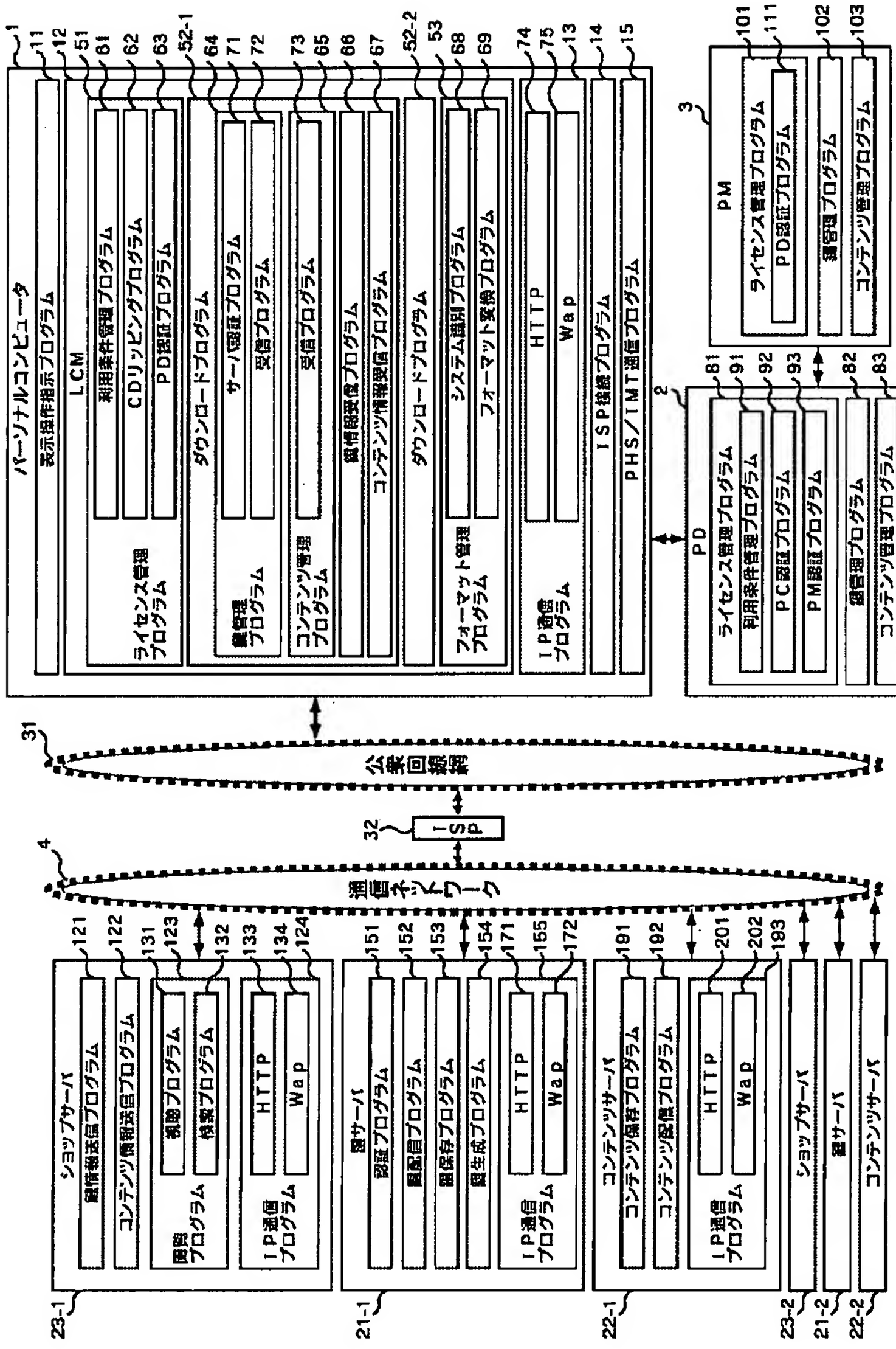
【図７】本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。

【図８】電話機一体型端末機５０１の構成を説明する図である。
【図９】代理サーバ５０３の構成を説明する図である。
【図１０】本願のデジタルデータ伝送システムの機能の構成を説明する図である。
【図１１】電話機一体型端末機５０１がサーバ５－１からコンテンツをダウンロードする処理を説明するフローチャートである。
【図１２】電話機一体型端末機５０１がサーバ５－１からコンテンツをダウンロードする処理を説明するフローチャートである。
【図１３】電話機一体型端末機５０１がサーバ５－２からコンテンツをダウンロードする処理を説明するフローチャートである。
【図１４】電話機一体型端末機５０１がサーバ５－２からコンテンツをダウンロードする処理を説明するフローチャートである。
【図１５】本願のデジタルデータ伝送システムの他の機能の構成を説明する図である。
【図１６】電話機一体型端末機５０１がサーバ５－２からコンテンツをダウンロードする処理を説明するフローチャートである。
【図１７】電話機一体型端末機５０１がサーバ５－２からコンテンツをダウンロードする処理を説明するフローチャートである。
【符号の説明】
５０１　電話機一体型端末機，　５０３　代理サーバ，　５１１　表示操作指示プログラム，　５１２　クライアント用ＬＣＭ，　５１４　サーバ用ＬＣＭ，６０１　ＣＰＵ，　６０２　ＲＯＭ，　６０３　ＲＡＭ，　６０８　通信部，６４１　磁気ディスク，　６４２　光ディスク，　６４３　光磁気ディスク，６４４　半導体メモリ，　６５１　ＣＰＵ，　６５２　ＲＯＭ，　６５３　ＲＡＭ，　６６３　通信部，　６８１　磁気ディスク，　６８２　光ディスク，６８３　光磁気ディスク，　６８４　半導体メモリ

【図１】

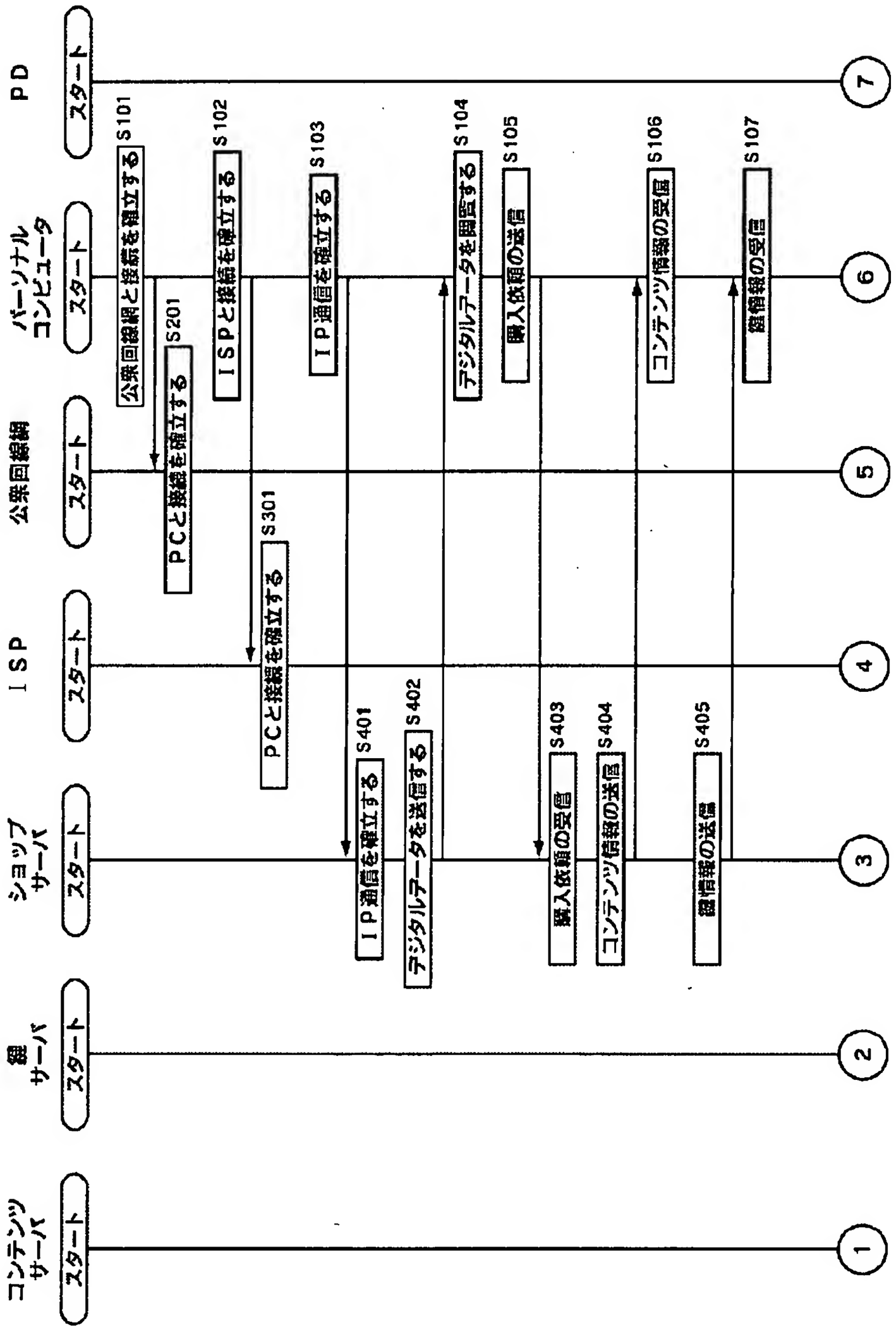


【図２】

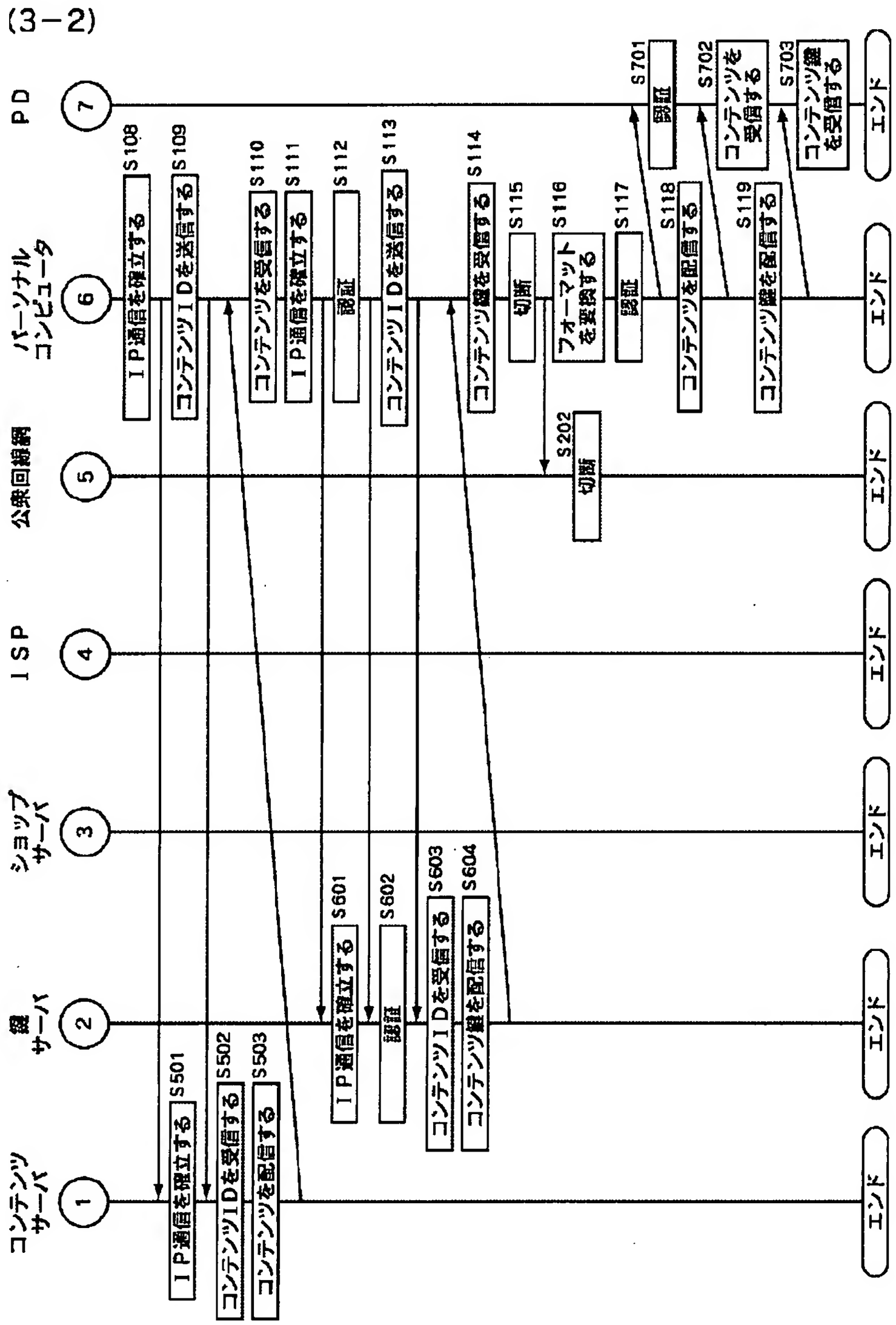

パーソナルコンピュータ
1
表示操作指示プログラム
11
LCM
12
ライセンス管理プログラム
51
利用条件管理プログラム
61
CDリッピングプログラム
62
PD認証プログラム
63
ダウンロードプログラム
52-1
署管理プログラム
64
サーバ認証プログラム
71
受信プログラム
72
コンテンツ管理プログラム
73
受信プログラム
65
鍵情報受信プログラム
66
コンテンツ情報受信プログラム
67
ダウンロードプログラム
52-2
フォーマット管理プログラム
53
システム識別プログラム
68
フォーマット変換プログラム
69
IP通信プログラム
74
HTTP
75
Wap
13
ISP接続プログラム
14
PHS／IMT通信プログラム
15
PM
3
ライセンス管理プログラム
101
利用条件管理プログラム
111
PD認証プログラム
102
鍵管理プログラム
103
コンテンツ管理プログラム
PD
2
ライセンス管理プログラム
81
利用条件管理プログラム
91
PC認証プログラム
92
PM認証プログラム
93
鍵管理プログラム
82
コンテンツ管理プログラム
83
公衆回線網
31
ISP
32
通信ネットワーク
4
121
122
131
123
132
133
134
124
151
152
153
154
171
155
172
191
192
201
202
193
ショップサーバ
鍵情報送信プログラム
コンテンツ情報送信プログラム
視聴プログラム
検索プログラム
鍵関連プログラム
HTTP
Wap
IP通信プログラム
23-1
鍵サーバ
認証プログラム
鍵配信プログラム
鍵保存プログラム
鍵生成プログラム
HTTP
Wap
IP通信プログラム
21-1
コンテンツサーバ
コンテンツ保存プログラム
コンテンツ配信プログラム
HTTP
Wap
IP通信プログラム
22-1
ショップサーバ
23-2
鍵サーバ
21-2
コンテンツサーバ
22-2

【図３】

(3－1)

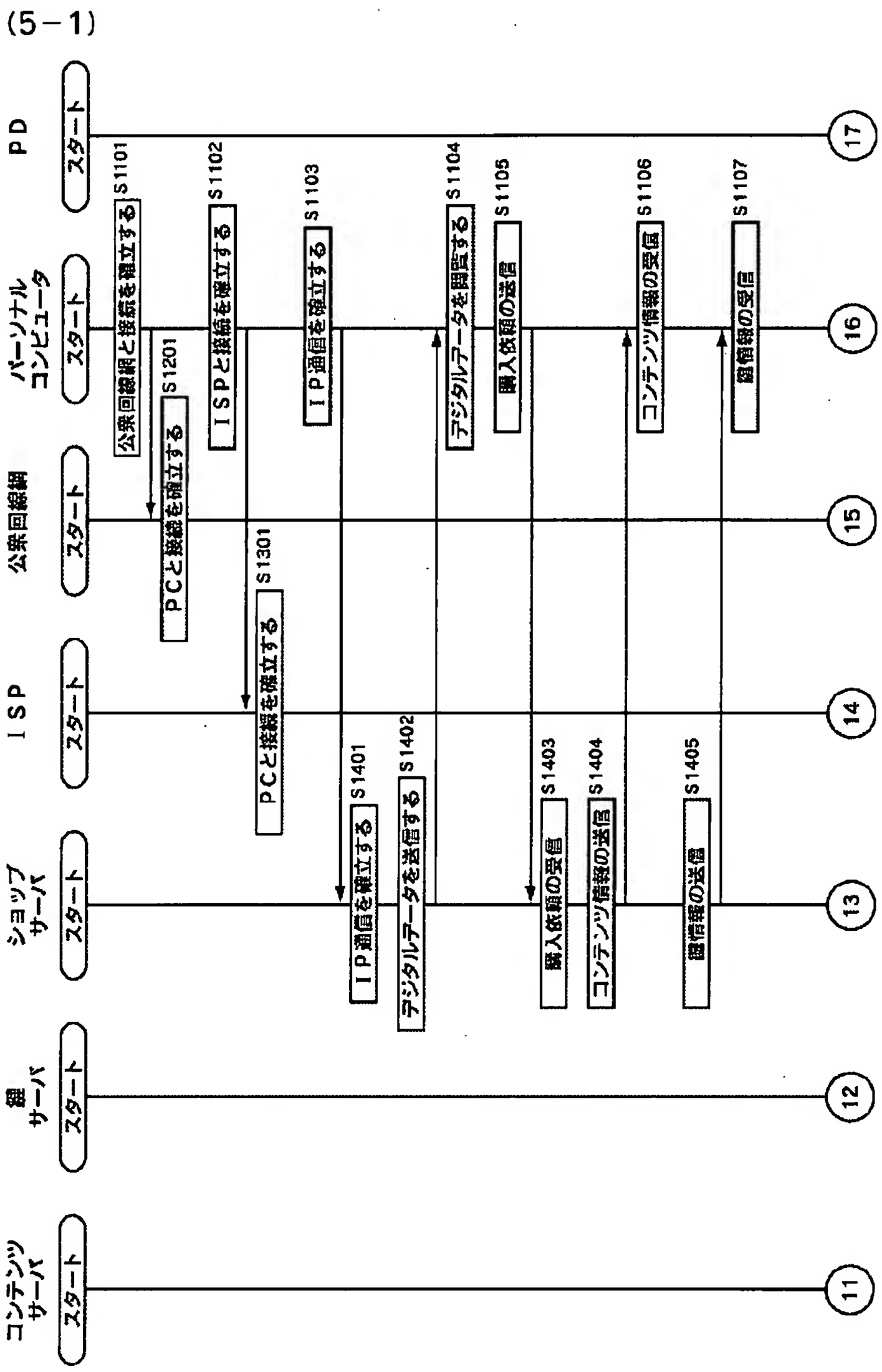

PD
パーソナル コンピュータ
公衆回線網
ISP
ショップ サーバ
鍵 サーバ
コンテンツ サーバ
スタート
S101
公衆回線網と接続を確立する
S201
PCと接続を確立する
S102
ISPと接続を確立する
S301
PCと接続を確立する
S103
IP通信を確立する
S401
IP通信を確立する
S402
デジタルデータを送信する
S104
デジタルデータを開錠する
S105
購入依頼の送信
S403
購入依頼の受信
S404
コンテンツ情報の送信
S106
コンテンツ情報の受信
S405
鍵情報の送信
S107
鍵情報の受信
1
2
3
4
5
6
7

【図４】

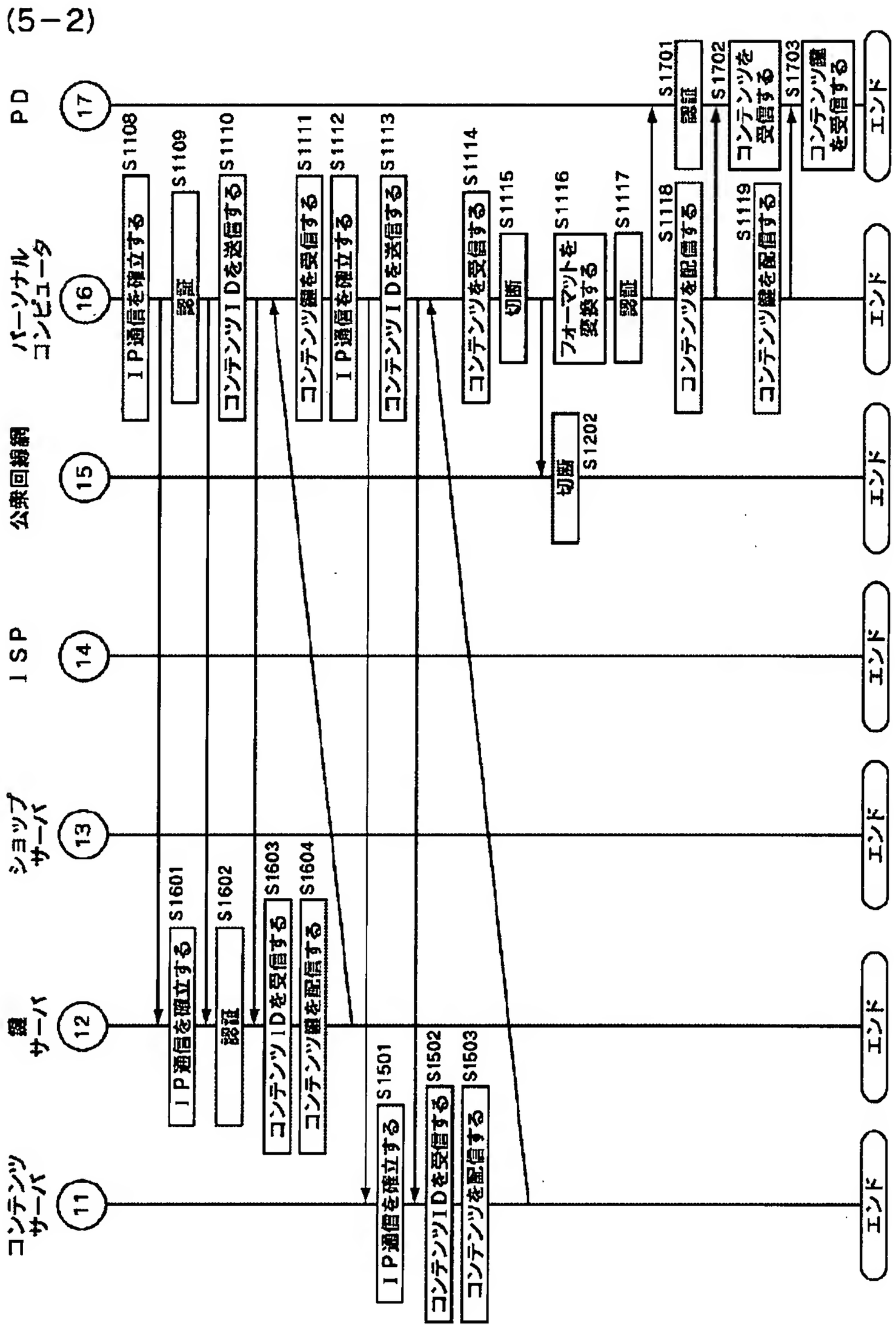

(3−2)
PD
パーソナル コンピュータ
公衆回線網
ISP
ショップ サーバ
銀 サーバ
コンテンツ サーバ
7
6
5
4
3
2
1
IP通信を確立する
コンテンツIDを送信する
コンテンツを受信する
IP通信を確立する
認証
コンテンツIDを送信する
コンテンツ鍵を受信する
切断
フォーマットを変換する
認証
認証
コンテンツを配信する
コンテンツ鍵を配信する
コンテンツを受信する
コンテンツ鍵を受信する
切断
IP通信を確立する
コンテンツIDを受信する
コンテンツを配信する
IP通信を確立する
認証
コンテンツIDを受信する
コンテンツ鍵を配信する
IP通信を確立する
コンテンツIDを受信する
コンテンツを配信する
S108
S109
S110
S111
S112
S113
S114
S115
S116
S117
S118
S119
S701
S702
S703
S202
S501
S502
S503
S601
S602
S603
S604
エンド

【図５】

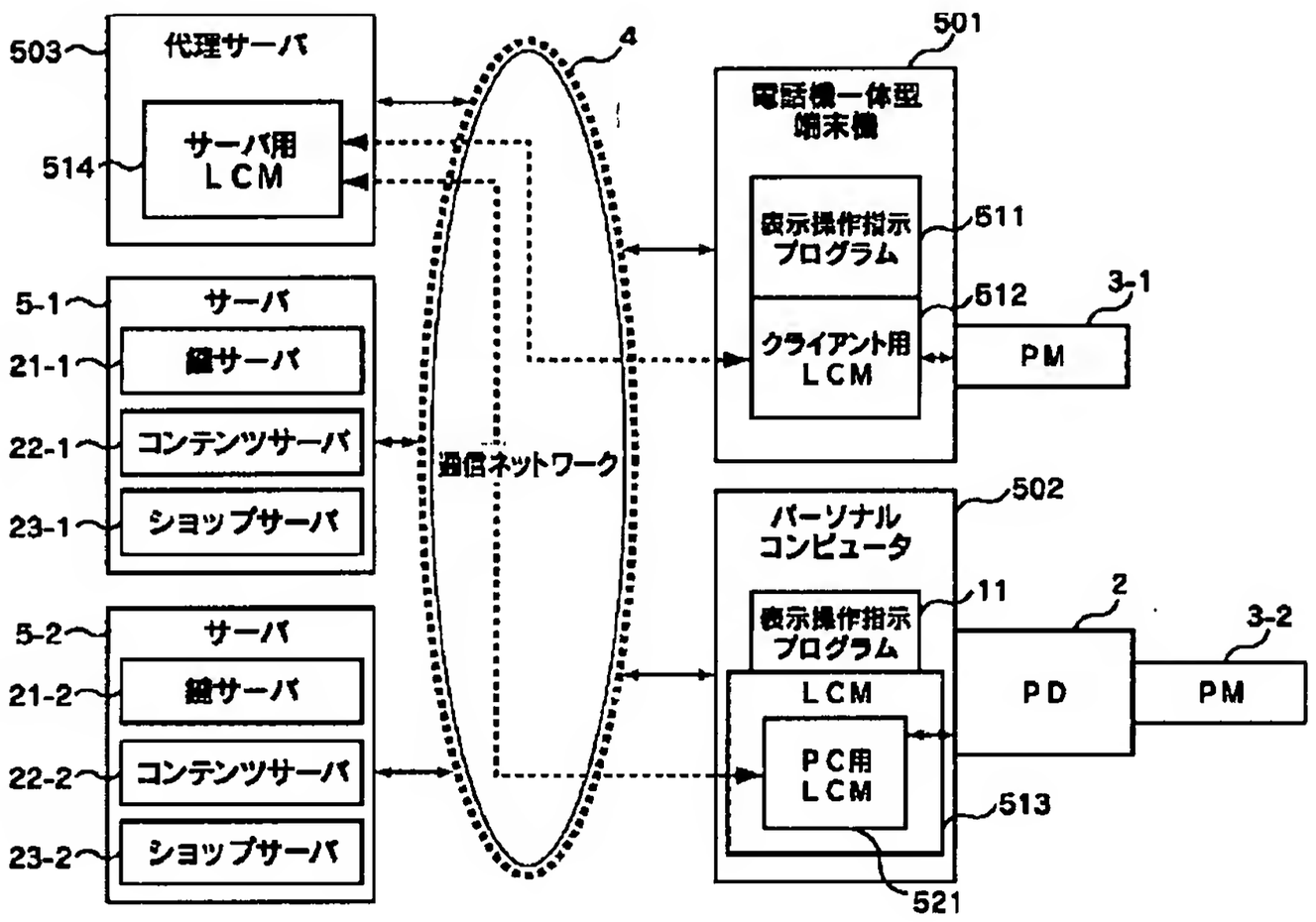
(5－1)


PD
パーソナル コンピュータ
公衆回線網
ISP
ショップ サーバ
銀 サーバ
コンテンツ サーバ
スタート
公衆回線網と接続を確立する
S1101
PCと接続を確立する
S1201
ISPと接続を確立する
S1102
IP通信を確立する
S1103
デジタルデータを閲覧する
S1104
購入依頼の送信
S1105
コンテンツ情報の受信
S1106
銀情報の受信
S1107
PCと接続を確立する
S1301
IP通信を確立する
S1401
デジタルデータを送信する
S1402
購入依頼の受信
S1403
コンテンツ情報の送信
S1404
銀情報の送信
S1405
17
16
15
14
13
12
11

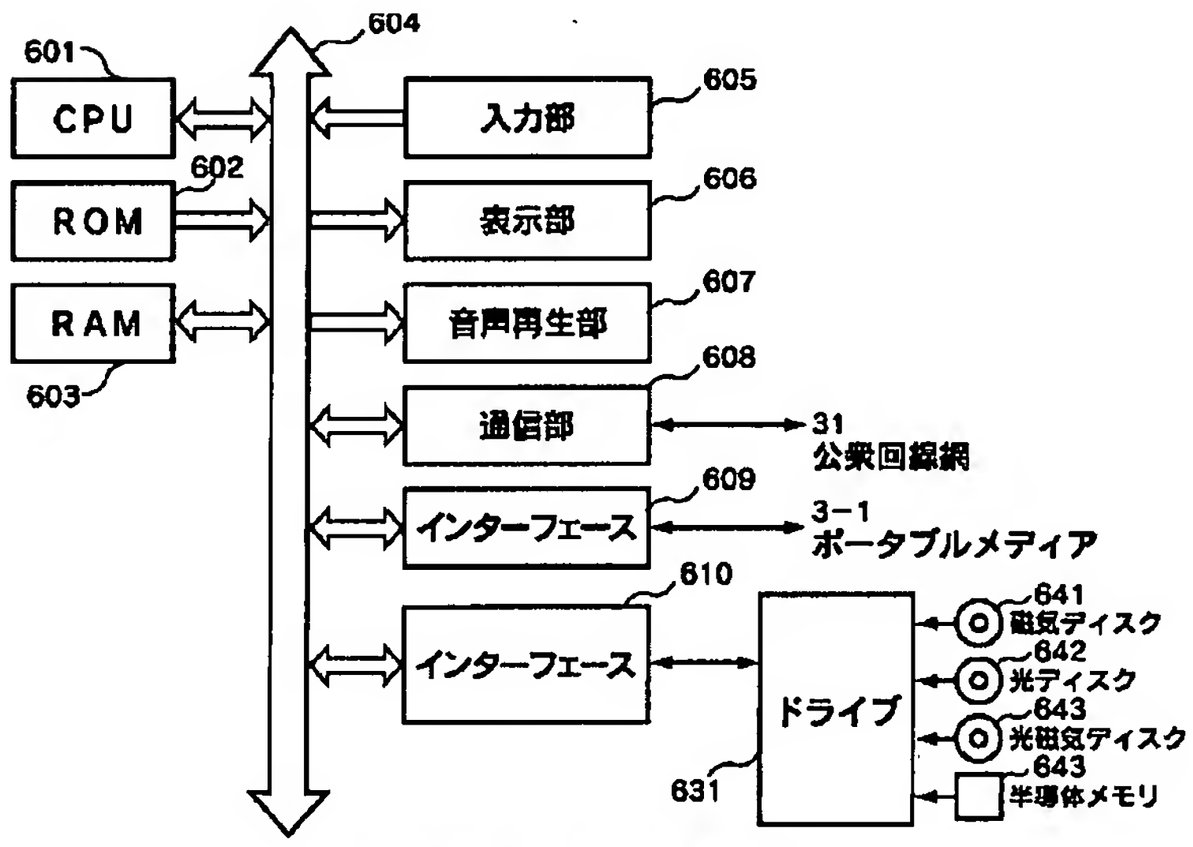
【図６】


(5－2)
PD
パーソナル コンピュータ
公衆回線網
ISP
ショップ サーバ
銀 サーバ
コンテンツ サーバ
17
16
15
14
13
12
11
IP通信を確立する
認証
コンテンツIDを送信する
コンテンツ鍵を受信する
IP通信を確立する
コンテンツIDを送信する
コンテンツを受信する
切断
フォーマットを 変換する
認証
認証
コンテンツを配信する
コンテンツ鍵を配信する
コンテンツを 受信する
コンテンツ鍵 を受信する
切断
エンド
S1108
S1109
S1110
S1111
S1112
S1113
S1114
S1115
S1116
S1117
S1118
S1119
S1202
S1701
S1702
S1703
IP通信を確立する
認証
コンテンツIDを受信する
コンテンツ鍵を配信する
S1601
S1602
S1603
S1604
IP通信を確立する
コンテンツIDを受信する
コンテンツを配信する
S1501
S1502
S1503

【図７】

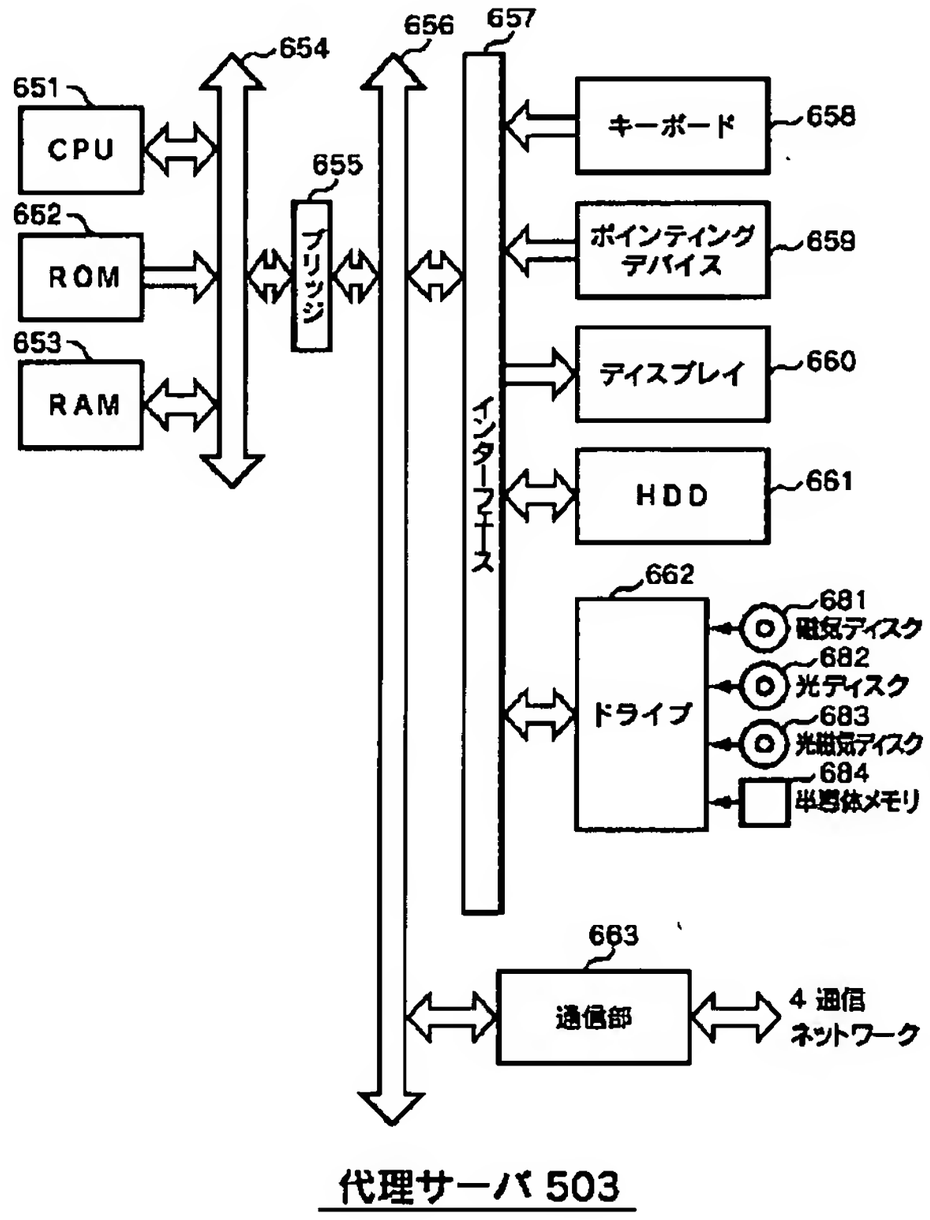



【図８】

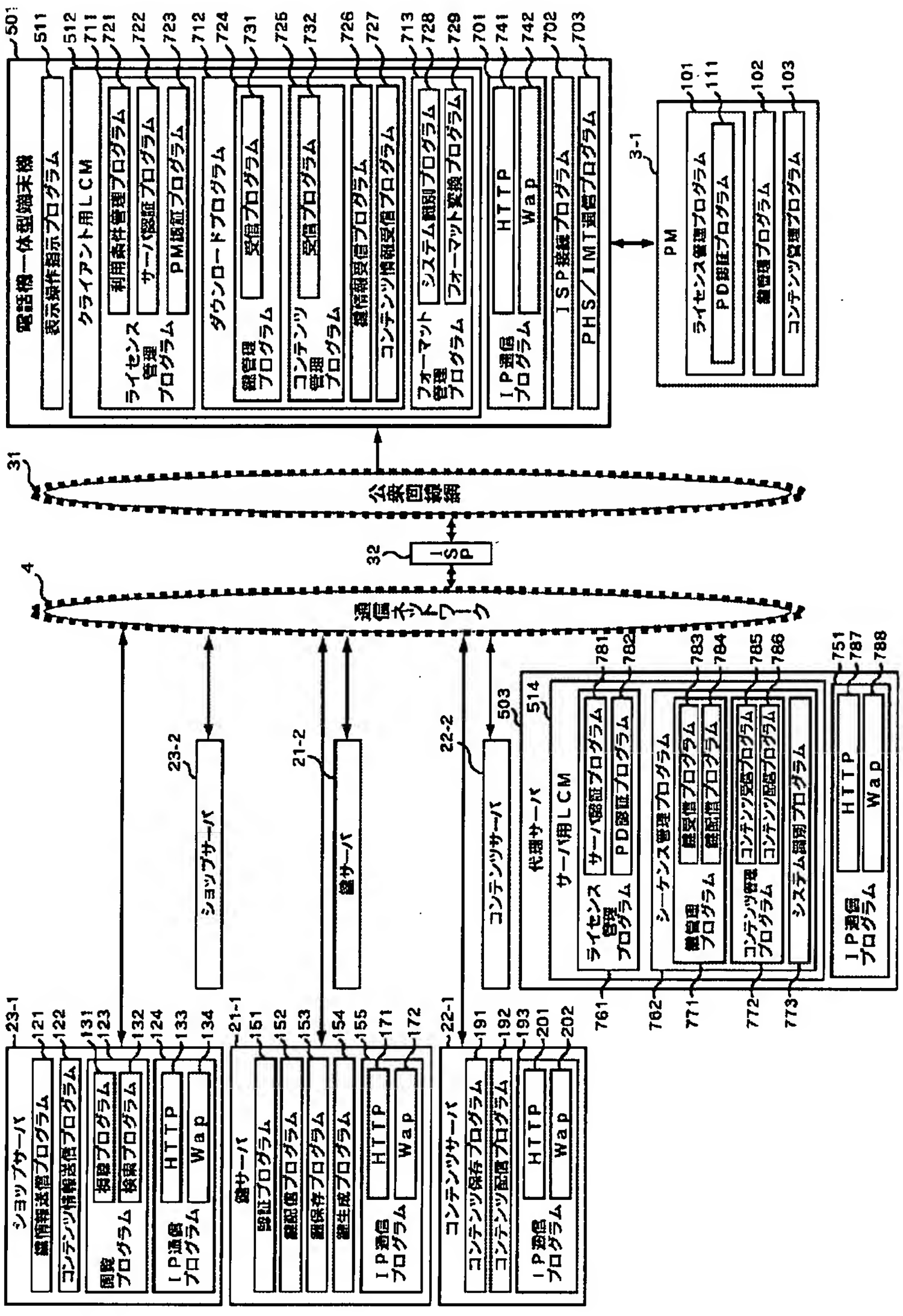



電話機一体型端末機 501

【図９】

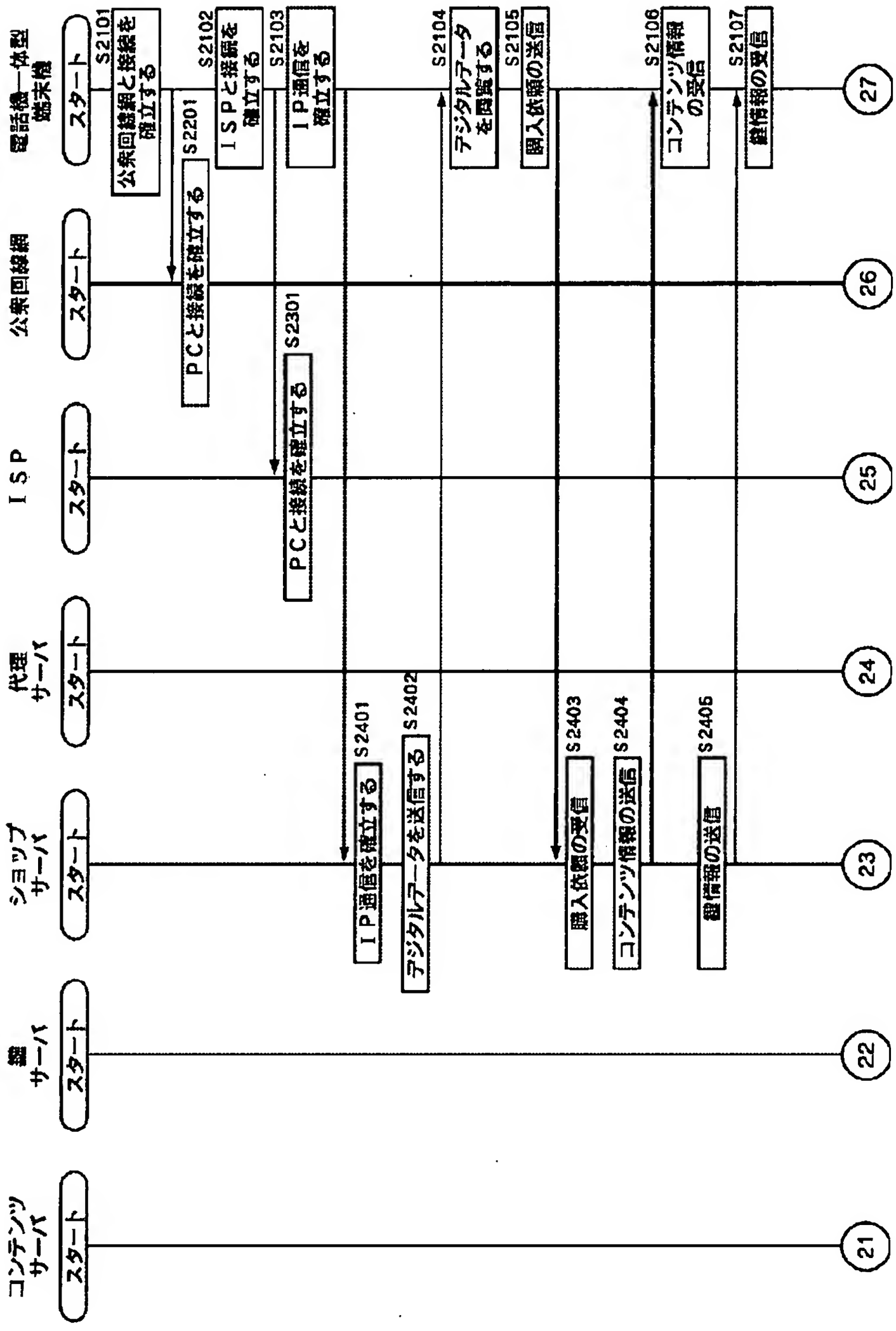

651
CPU
652
ROM
653
RAM
654
655
ブリッジ
656
657
インターフェース
キーボード
658
ポインティングデバイス
659
ディスプレイ
660
HDD
661
662
ドライブ
681
磁気ディスク
682
光ディスク
683
光磁気ディスク
684
半導体メモリ
663
通信部
4 通信ネットワーク
代理サーバ 503

【図１０】


電話機一体型端末機
501
表示操作指示プログラム
511
クライアント用LCM
512
ライセンス管理プログラム
利用条件管理プログラム
711
721
サーバ認証プログラム
722
PM認証プログラム
723
712
ダウンロードプログラム
724
鍵管理プログラム
受信プログラム
731
725
コンテンツ管理プログラム
受信プログラム
732
726
鍵情報受信プログラム
727
コンテンツ情報受信プログラム
713
フォーマット管理プログラム
システム識別プログラム
728
フォーマット変換プログラム
729
701
IP通信プログラム
HTTP
741
Wap
742
ISP接続プログラム
702
PHS／IMT通信プログラム
703
3-1
PM
101
ライセンス管理プログラム
111
PD認証プログラム
102
鍵管理プログラム
103
コンテンツ管理プログラム
31
公衆回線網
32
ISP
4
通信ネットワーク
23-2
ショップサーバ
21-2
鍵サーバ
22-2
コンテンツサーバ
503
514
代理サーバ
サーバ用LCM
ライセンス管理プログラム
サーバ認証プログラム
781
PD認証プログラム
782
シーケンス管理プログラム
鍵受信プログラム
783
鍵配信プログラム
784
コンテンツ管理プログラム
コンテンツ受信プログラム
785
コンテンツ配信プログラム
786
システム識別プログラム
IP通信プログラム
HTTP
751
Wap
787
788
761
762
771
772
773
23-1
ショップサーバ
鍵情報送信プログラム
121
コンテンツ情報送信プログラム
122
閲覧プログラム
鍵閲覧プログラム
131
検索プログラム
123
IP通信プログラム
HTTP
132
Wap
124
133
134
21-1
鍵サーバ
鍵認証プログラム
151
鍵配信プログラム
152
鍵保存プログラム
153
鍵生成プログラム
154
IP通信プログラム
HTTP
155
Wap
171
172
22-1
コンテンツサーバ
コンテンツ保存プログラム
191
コンテンツ配信プログラム
192
IP通信プログラム
HTTP
193
Wap
201
202

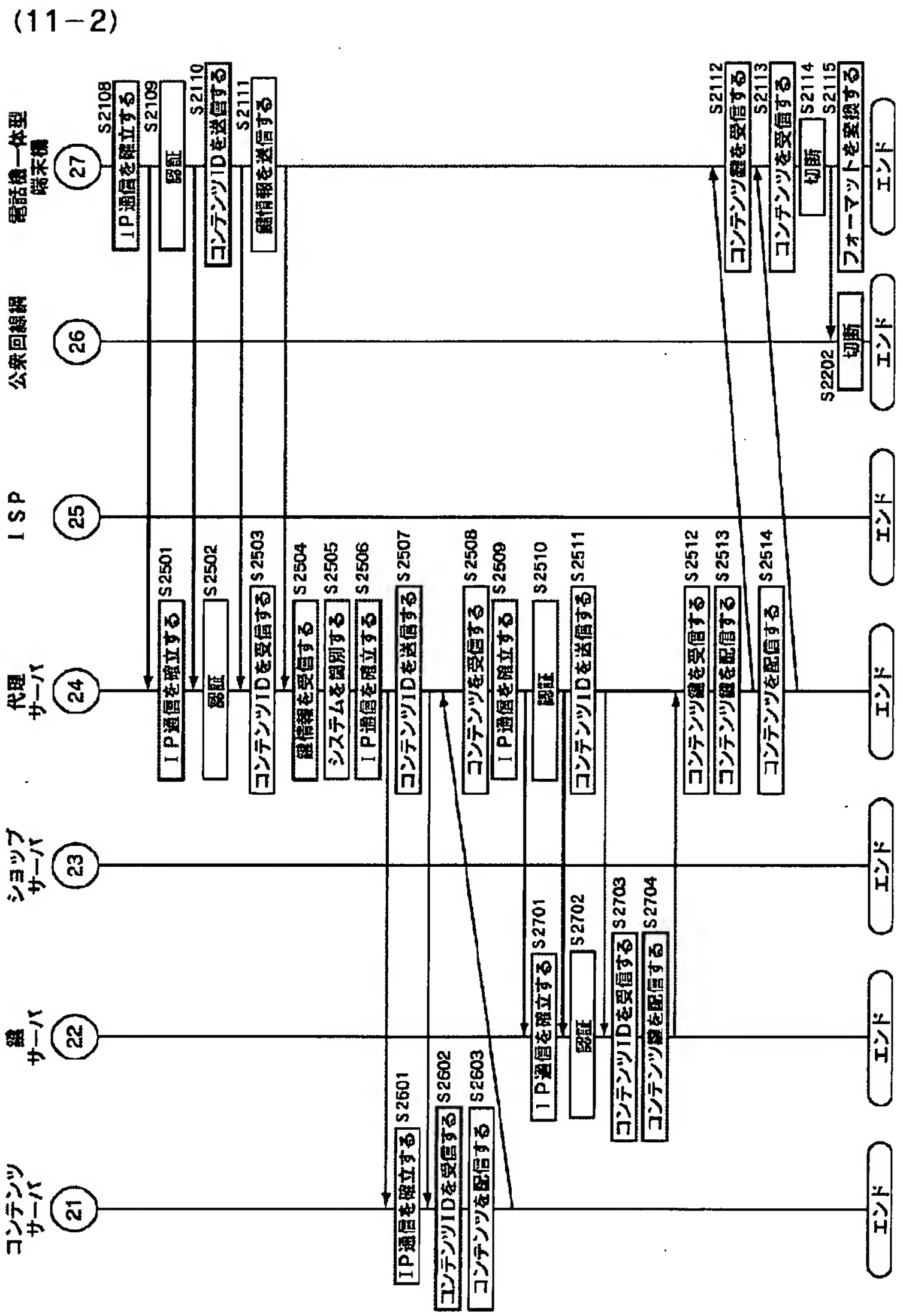
【図１１】

(11－1)


電話機一体型端末機
公衆回線網
ISP
ショップサーバ
代理サーバ
コンテンツサーバ
スタート
S2101
公衆回線網と接続を確立する
S2102
ISPと接続を確立する
S2103
IP通信を確立する
S2104
デジタルデータを問監する
S2105
購入依頼の送信
S2106
コンテンツ情報の受信
S2107
確情報の受信
S2201
PCと接続を確立する
S2301
PCと接続を確立する
S2401
IP通信を確立する
S2402
デジタルデータを送信する
S2403
購入依頼の受信
S2404
コンテンツ情報の送信
S2405
確情報の送信
21
22
23
24
25
26
27

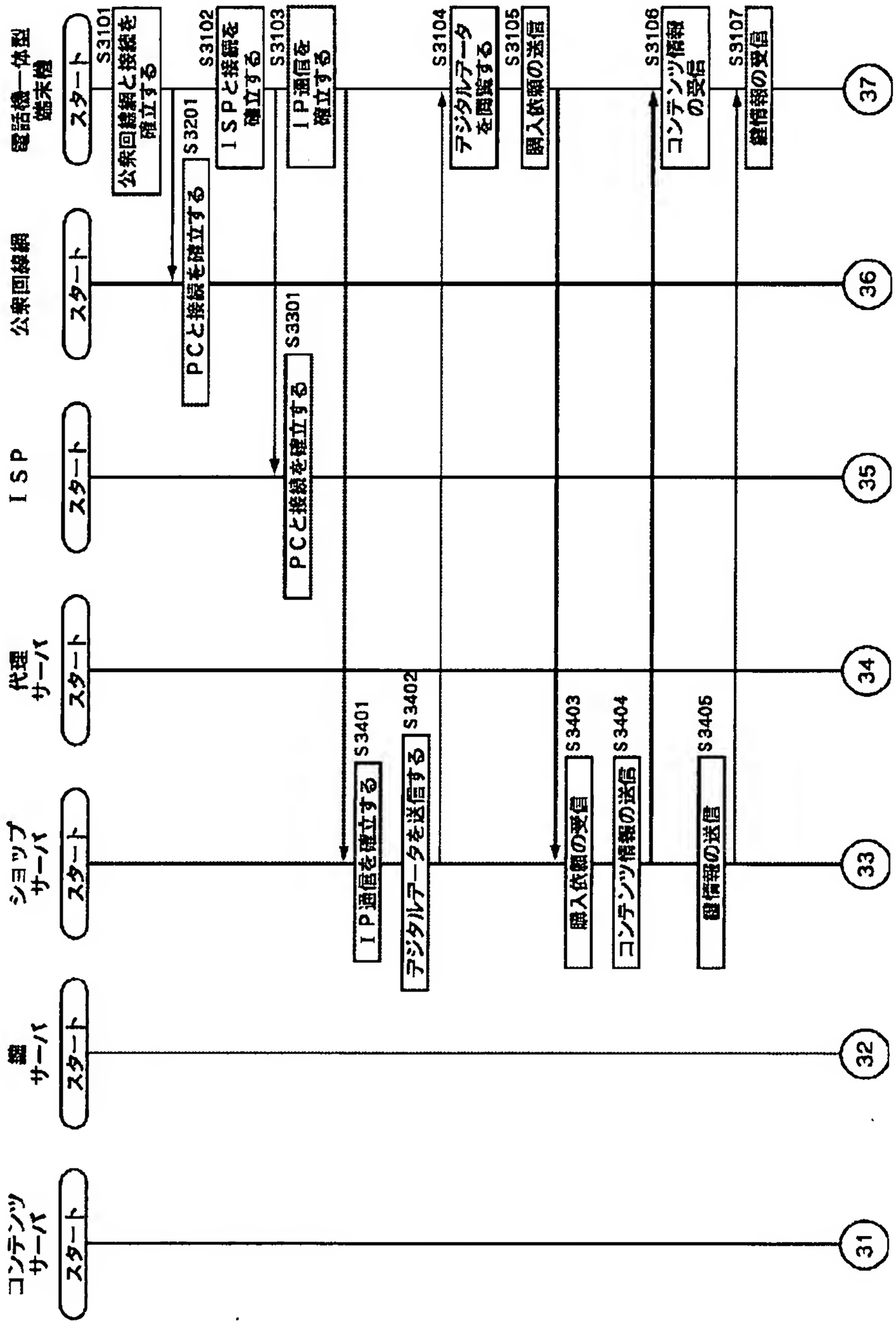
【図１２】

(11−2)

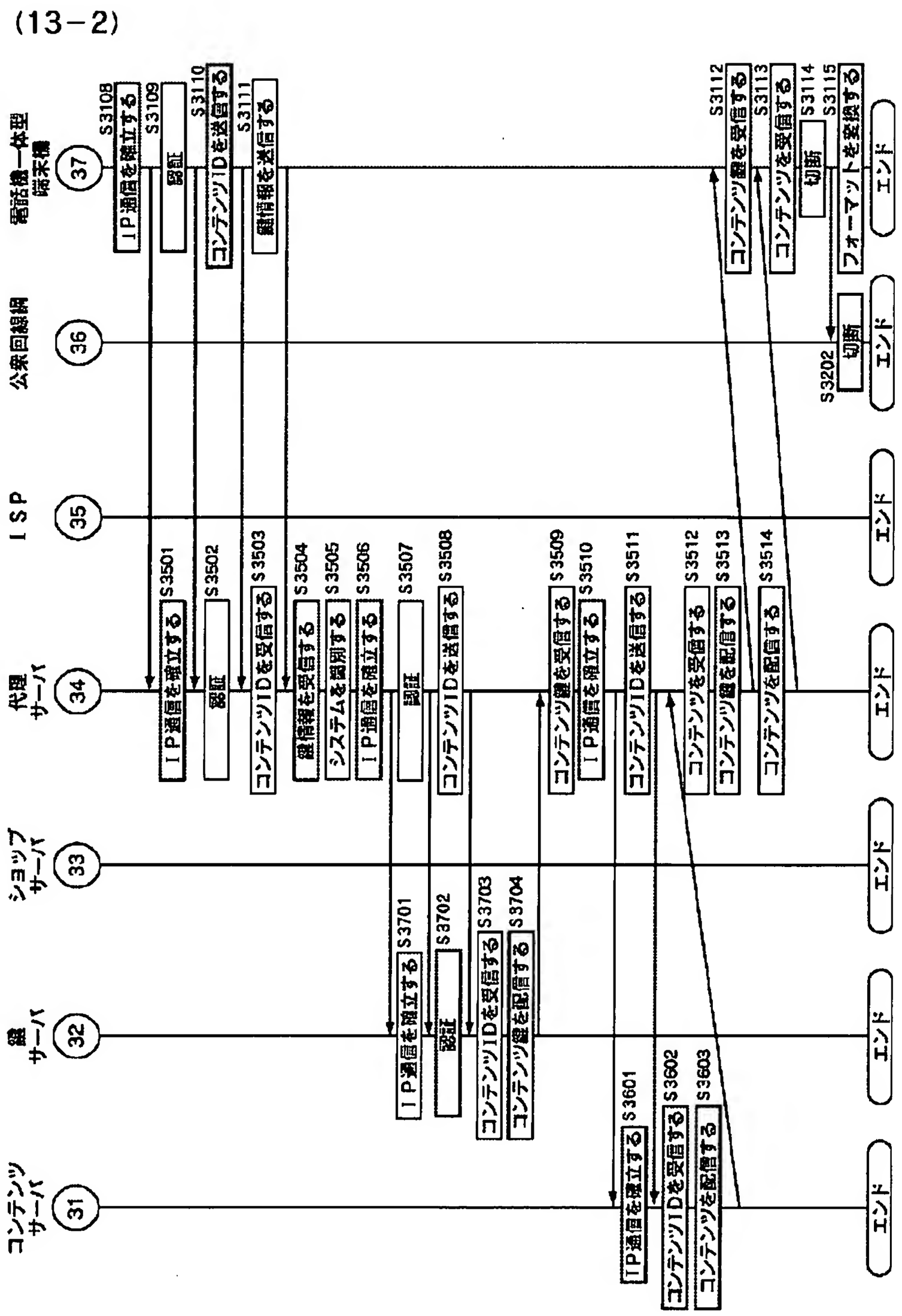

電話機一体型端末機
公衆回線網
ISP
代理サーバ
ショップサーバ
鍵サーバ
コンテンツサーバ
27
26
25
24
23
22
21
IP通信を確立する
認証
コンテンツIDを送信する
鍵情報を送信する
S2108
S2109
S2110
S2111
S2112
コンテンツ鍵を受信する
S2113
コンテンツを受信する
S2114
切断
S2115
フォーマットを変換する
エンド
S2202
切断
エンド
IP通信を確立する
S2501
認証
S2502
コンテンツIDを受信する
S2503
鍵情報を受信する
S2504
システムを閉鎖する
S2505
IP通信を確立する
S2506
コンテンツIDを送信する
S2507
コンテンツを受信する
S2508
IP通信を確立する
S2509
認証
S2510
コンテンツIDを送信する
S2511
コンテンツ鍵を受信する
S2512
コンテンツ鍵を配信する
S2513
コンテンツを配信する
S2514
エンド
エンド
エンド
IP通信を確立する
S2601
コンテンツIDを受信する
S2602
コンテンツを配信する
S2603
IP通信を確立する
S2701
認証
S2702
コンテンツIDを受信する
S2703
コンテンツ鍵を配信する
S2704
エンド
IP通信を確立する
コンテンツIDを受信する
コンテンツを配信する
エンド

【図１３】

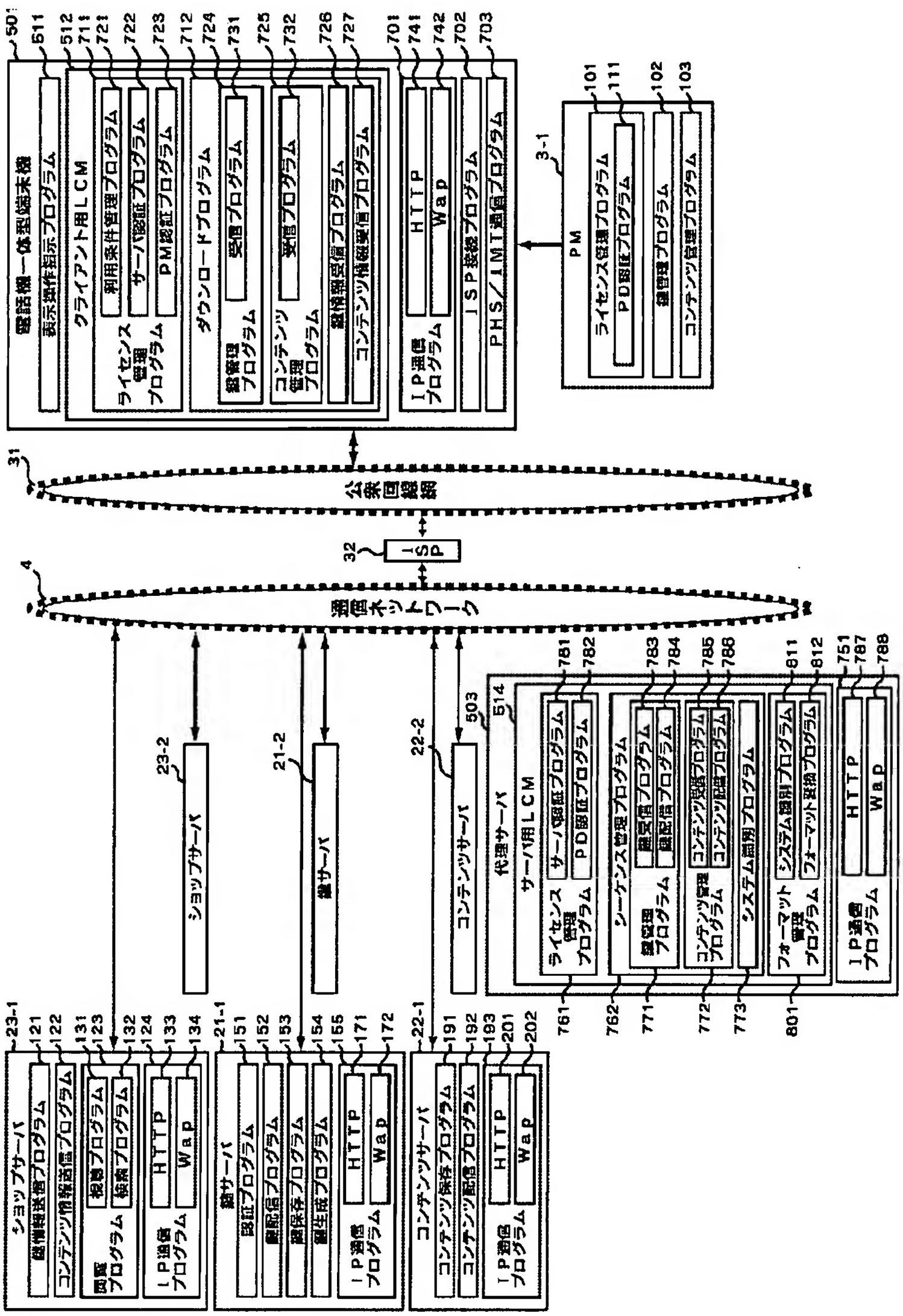
(13－1)


電話機一体型端末機
公衆回線網
ISP
代理サーバ
ショップサーバ
コンテンツサーバ
スタート
S3101
公衆回線網と接続を確立する
S3102
ISPと接続を確立する
S3103
IP通信を確立する
S3104
デジタルデータを同旋する
S3105
購入依頼の送信
S3106
コンテンツ情報の受信
S3107
確情報の受信
S3201
PCと接続を確立する
S3301
PCと接続を確立する
S3401
IP通信を確立する
S3402
デジタルデータを送信する
S3403
購入依頼の受信
S3404
コンテンツ情報の送信
S3405
確情報の送信
31
32
33
34
35
36
37

【図１４】

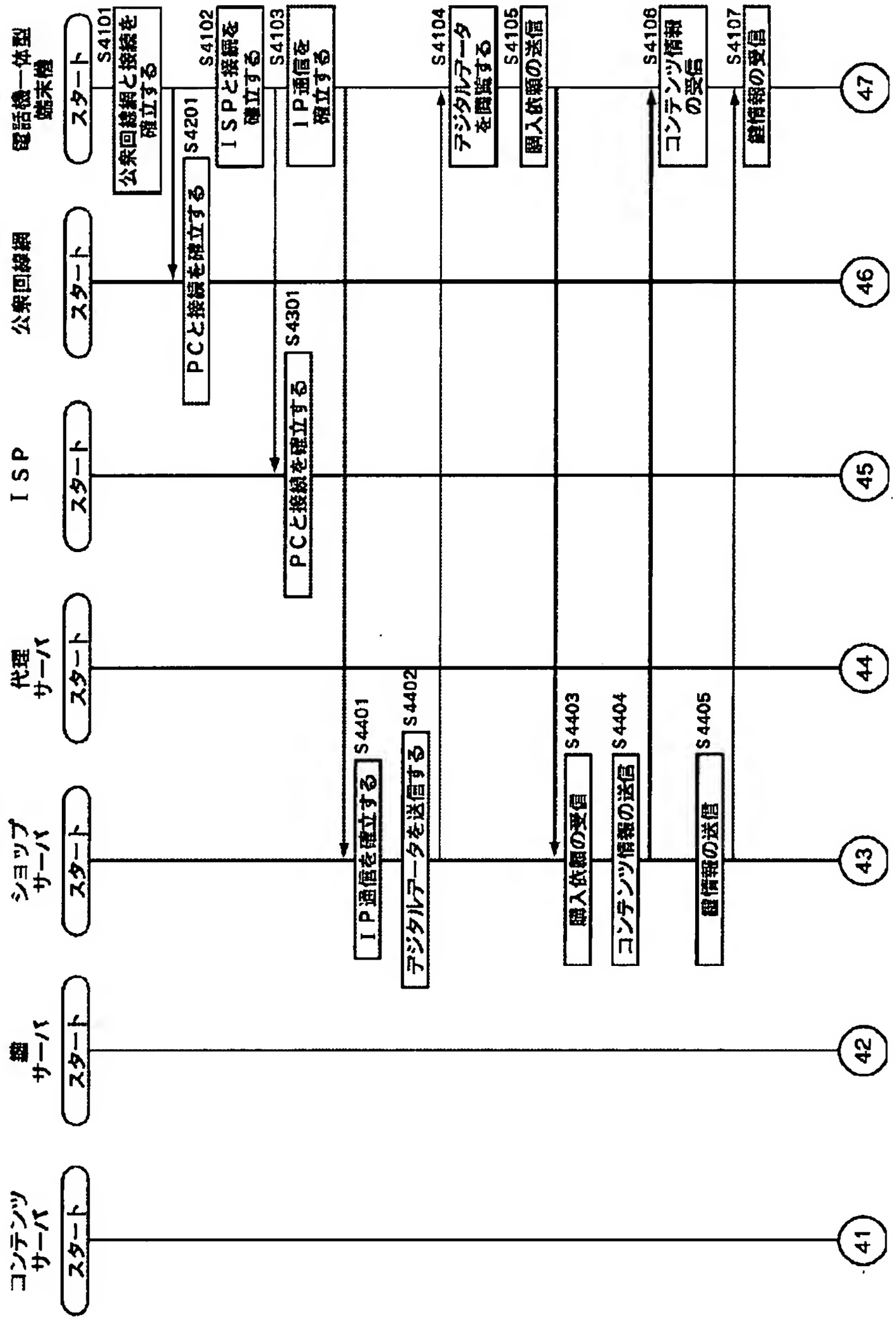

(13-2)
電話機一体型端末機
37
公衆回線網
36
ISP
35
代理サーバ
34
ショップサーバ
33
鍵サーバ
32
コンテンツサーバ
31
S3108
IP通信を確立する
S3109
認証
S3110
コンテンツIDを送信する
S3111
鍵情報を送信する
S3112
コンテンツ鍵を受信する
S3113
コンテンツを受信する
S3114
切断
S3115
フォーマットを変換する
エンド
S3202
切断
エンド
S3501
IP通信を確立する
S3502
認証
S3503
コンテンツIDを受信する
S3504
鍵情報を受信する
S3505
システムを認別する
S3506
IP通信を確立する
S3507
認証
S3508
コンテンツIDを送信する
S3509
コンテンツ鍵を受信する
S3510
IP通信を確立する
S3511
コンテンツIDを送信する
S3512
コンテンツを受信する
S3513
コンテンツ鍵を配信する
S3514
コンテンツを配信する
エンド
S3701
IP通信を確立する
S3702
認証
S3703
コンテンツIDを受信する
S3704
コンテンツ鍵を配信する
S3601
IP通信を確立する
S3602
コンテンツIDを受信する
S3603
コンテンツを配信する
エンド

【図１５】

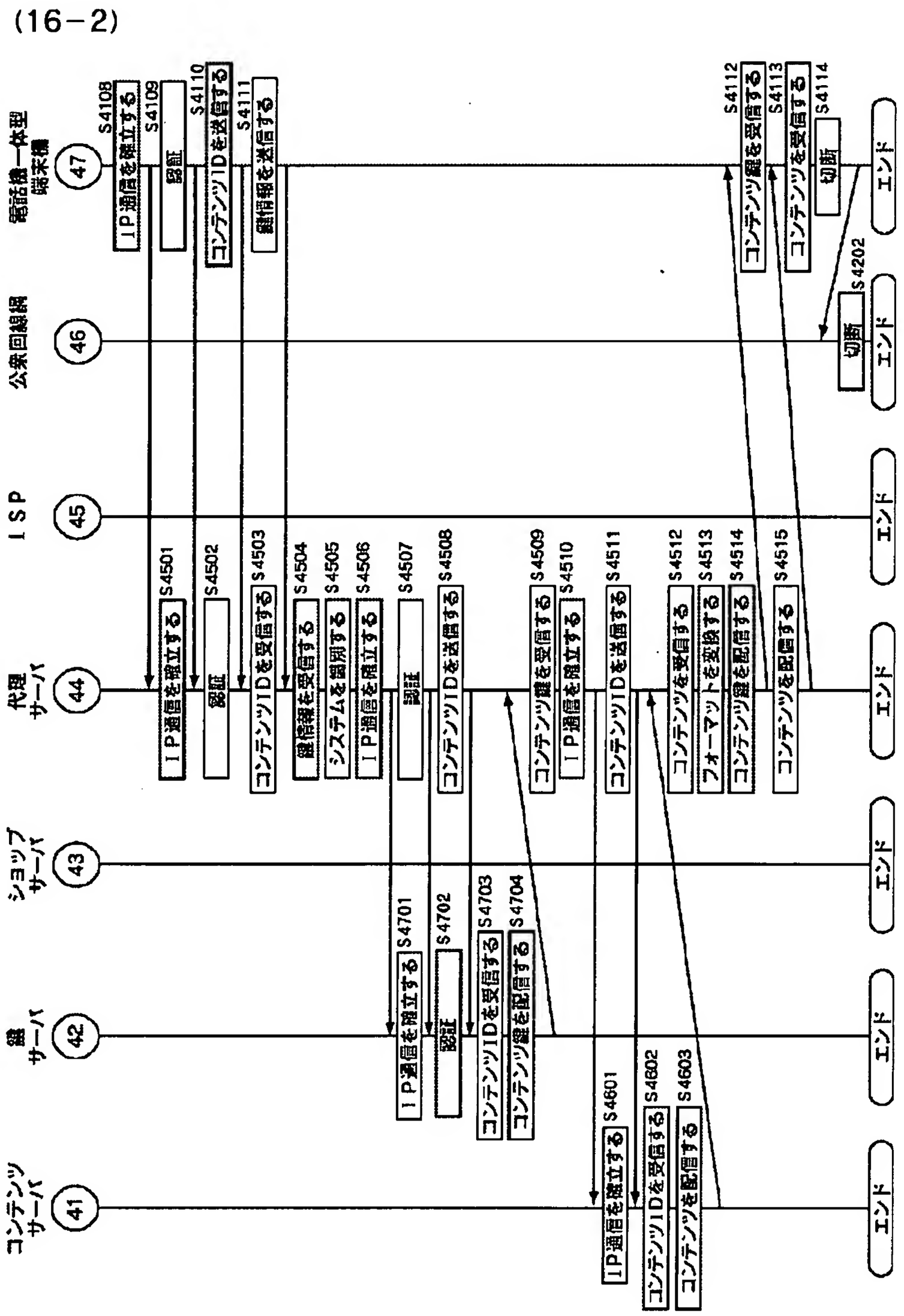

501
電話機一体型端末機
511
表示操作指示プログラム
512
クライアント用ＬＣＭ
711
ライセンス管理プログラム
721
利用条件管理プログラム
722
サーバ認証プログラム
723
ＰＭ認証プログラム
712
ダウンロードプログラム
724
鍵管理プログラム
731
受信プログラム
725
コンテンツ管理プログラム
732
受信プログラム
726
鍵情報受信プログラム
727
コンテンツ情報受信プログラム
701
ＩＰ通信プログラム
741
ＨＴＴＰ
742
Ｗａｐ
702
ＩＳＰ接続プログラム
703
ＰＨＳ／ＩＭＴ通信プログラム
3-1
ＰＭ
101
ライセンス管理プログラム
111
ＰＤ認証プログラム
102
鍵管理プログラム
103
コンテンツ管理プログラム
31
公衆回線網
32
ＩＳＰ
4
通信ネットワーク
23-2
ショップサーバ
21-2
鍵サーバ
22-2
コンテンツサーバ
503
514
代理サーバ
サーバ用ＬＣＭ
781
ライセンス管理プログラム
サーバ認証プログラム
782
ＰＤ認証プログラム
783
シーケンス管理プログラム
鍵受信プログラム
784
鍵配信プログラム
785
コンテンツ受信プログラム
786
コンテンツ配信プログラム
811
システム識別プログラム
812
フォーマット変換プログラム
751
ＩＰ通信プログラム
787
ＨＴＴＰ
788
Ｗａｐ
761
762
771
772
773
801
23-1
ショップサーバ
121
鍵情報送信プログラム
122
コンテンツ情報送信プログラム
131
閲覧プログラム
123
視聴プログラム
132
検索プログラム
124
ＩＰ通信プログラム
133
ＨＴＴＰ
134
Ｗａｐ
21-1
鍵サーバ
151
認証プログラム
152
鍵配信プログラム
153
鍵保存プログラム
154
鍵生成プログラム
155
ＩＰ通信プログラム
171
ＨＴＴＰ
172
Ｗａｐ
22-1
コンテンツサーバ
191
コンテンツ保存プログラム
192
コンテンツ配信プログラム
193
ＩＰ通信プログラム
201
ＨＴＴＰ
202
Ｗａｐ

【図１６】

(16－1)


電話機一体型端末機
公衆回線網
ISP
代理サーバ
ショップサーバ
コンテンツサーバ
スタート
S4101
公衆回線網と接続を確立する
S4102
ISPと接続を確立する
S4103
IP通信を確立する
S4104
デジタルデータを問監する
S4105
購入依頼の送信
S4106
コンテンツ情報の受信
S4107
確情報の受信
S4201
PCと接続を確立する
S4301
PCと接続を確立する
S4401
IP通信を確立する
S4402
デジタルデータを送信する
S4403
購入依頼の受信
S4404
コンテンツ情報の送信
S4405
確情報の送信
41
42
43
44
45
46
47

【図１７】


(16−2)
電話機一体型端末機
公衆回線網
ISP
代理サーバ
ショップサーバ
鍵サーバ
コンテンツサーバ
47
46
45
44
43
42
41
S4108
IP通信を確立する
S4109
認証
S4110
コンテンツIDを送信する
S4111
鍵情報を送信する
S4112
コンテンツ鍵を受信する
S4113
コンテンツを受信する
S4114
切断
エンド
S4202
切断
エンド
S4501
IP通信を確立する
S4502
認証
S4503
コンテンツIDを受信する
S4504
鍵情報を受信する
S4505
システムを留保する
S4506
IP通信を確立する
S4507
認証
S4508
コンテンツIDを送信する
S4509
コンテンツ鍵を受信する
S4510
IP通信を確立する
S4511
コンテンツIDを送信する
S4512
コンテンツを受信する
S4513
フォーマットを変換する
S4514
コンテンツ鍵を配信する
S4515
コンテンツを配信する
エンド
エンド
エンド
エンド
S4701
IP通信を確立する
S4702
認証
S4703
コンテンツIDを受信する
S4704
コンテンツ鍵を配信する
S4601
IP通信を確立する
S4602
コンテンツIDを受信する
S4603
コンテンツを配信する
エンド

PATENT ABSTRACTS OF JAPAN
(11)Publication number : 2001-265361
(43)Date of publication of application : 28.09.2001
(51)Int.Cl. G10K 15/04
H04L 9/08
(21)Application number : 2000-070461 (71)Applicant : SONY CORP
(22)Date of filing : 14.03.2000 (72)Inventor : GO NAOMI
KURIHARA AKIRA
(54) DEVICE AND METHOD FOR PROVIDING INFORMATION, DEVICE AND METHOD FOR PROVIDING INFORMATION, AND PROGRAM STORAGE MEDIUM
(57)Abstract:
PROBLEM TO BE SOLVED: To receive contents and keys supplied by different procedures.
SOLUTION: A license managing program 761 authenticates a telephone set integrated type terminal machine 501 and also authenticates a 1st or 2nd server. An LCM 514 for the servers controls requests the transmission of the contents and keys and controls the reception of data specifying the 1st server or data specifying the 2nd server, and controls communication so that the contents and keys are received from the 1st server by the procedure corresponding to the 1st server when the data specifying the 1st server are received or from the 2nd server by the procedure corresponding to the 2nd server when the data specifying the 2nd server are received. The LCM 514 for the servers controls the transmission of the contents and keys to the telephone set integrated type terminal machine 501.
LEGAL STATUS [Date of request for examination] 28.02.2007
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]
* NOTICES *

CLAIMS
[Claim(s)]
[Claim 1] The 1st authentication means which attests the 1st information processor, and the 2nd authentication means which attests the 2nd information processor or 3rd information processor, A reception-control means to control the reception of data which specifies the data which specify said 2nd information processor as the Request to Send

of the contents and the key from said 1st information processor, and a list, or said 3rd information processor, When said data which specify said 2nd information processor are received, in the procedure corresponding to said 2nd information processor While transmitting the Request to Send of said contents and said key to said 2nd information processor When said contents and said key are received from said 2nd information processor and said data which specify said 3rd information processor are received, in the procedure corresponding to said 3rd information processor While transmitting the Request to Send of said contents and said key to said 3rd information processor Information offer equipment characterized by including a communications control means to control a communication link to receive said contents and said key from said 3rd information processor, and a transmission-control means to control said contents to said 1st information processor, and transmission of said key.

[Claim 2] Information offer equipment according to claim 1 characterized by including further a conversion means to transform either [ at least ] the coding method of said contents, or the cipher systems into a predetermined coding method or a predetermined cipher system.

[Claim 3] The 1st authentication step which attests the 1st information processor, and the 2nd authentication step which attests the 2nd information processor or 3rd information processor, The reception-control step which controls the reception of data which specifies the data which specify said 2nd information processor as the Request to Send of the contents and the key from said 1st information processor, and a list, or said 3rd information processor, When said data which specify said 2nd information processor are received, in the procedure corresponding to said 2nd information processor While transmitting the Request to Send of said contents and said key to said 2nd information processor When said contents and said key are received from said 2nd information processor and said data which specify said 3rd information processor are received, in the procedure corresponding to said 3rd information processor While transmitting the Request to Send of said contents and said key to said 3rd information processor The information offer approach characterized by including the communications control step which controls a communication link to receive said contents and said key from said 3rd information processor, and the transmission-control step which controls said contents to said 1st information processor, and transmission of said key.

[Claim 4] The 1st authentication step which attests the 1st information processor, and the 2nd authentication step which attests the 2nd information processor or 3rd information processor, The reception-control step which controls the reception of data which specifies the data which specify said 2nd information processor as the Request to Send of the contents and the key from said 1st information processor, and a list, or said 3rd information processor, When said data which specify said 2nd information processor are received, in the procedure corresponding to said 2nd information processor While transmitting the Request to Send of said contents and said key to said 2nd information processor When said contents and said key are received from said 2nd information processor and said data which specify said 3rd information processor are received, in the procedure corresponding to said 3rd information processor While transmitting the Request to Send of said contents and said key to said 3rd information processor The communications control step which controls a communication link to

receive said contents and said key from said 3rd information processor, The program storing medium by which the program which the computer characterized by including the transmission-control step which controls said contents to said 1st information processor and transmission of said key can read is stored.
[Claim 5] An authentication means to attest the 1st information offer equipment, and said 1st information offer equipment, Contents and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with said contents and said key, And a transmission-control means to control transmission of either of the data which specifies the 3rd information offer equipment which offers said contents and said key, The information processor characterized by including a reception-control means for said 1st information offer equipment to receive offer from said 2nd information offer equipment or said 3rd information offer equipment, and to control reception of said contents which transmitted, and said key.
[Claim 6] The authentication step which attests the 1st information offer equipment, and said 1st information offer equipment, Contents and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with said contents and said key, And the transmission-control step which controls transmission of either of the data which specifies the 3rd information offer equipment which offers said contents and said key, The information processing approach characterized by including the reception-control step which said 1st information offer equipment receives offer from said 2nd information offer equipment or said 3rd information offer equipment, and controls reception of said contents which transmitted, and said key.
[Claim 7] The authentication step which attests the 1st information offer equipment, and said 1st information offer equipment, Contents and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with said contents and said key, And the transmission-control step which controls transmission of either of the data which specifies the 3rd information offer equipment which offers said contents and said key, Said 1st information offer equipment receives offer from said 2nd information offer equipment or said 3rd information offer equipment. The program storing medium by which the program which the computer characterized by including the reception-control step which controls reception of said contents which transmitted, and said key can read is stored.
DETAILED DESCRIPTION
[Detailed Description of the Invention]
[0001]
[Field of the Invention] Especially this invention relates to a program storing medium at the information offer equipment and the approach of using the contents which offer the key which decodes contents and contents about a program storing medium in information offer equipment and an approach, an information processor and an approach, and a list, or are enciphered, an information processor and an approach, and a list.
[0002]
[Description of the Prior Art] Drawing 1 is drawing showing the configuration of the conventional digital data transmission system. The personal computer 1 is connected to the communication network 4 which consists of a Local Area Network or the Internet. With cipher systems, such as DES (Data Encryption Standard), it enciphers and a

personal computer 1 is recorded while it changes into the method (for example, ATRAC3 (trademark)) of predetermined compression the data (contents are called hereafter) of the musical sound which received from the contents server 22-1 or 22-2, or was read in CD (Compact Disc).
[0003] A personal computer 1 records the data of use conditions in which the use conditions of contents are shown corresponding to the contents currently enciphered and recorded.
[0004] The data of use conditions show the number (number of the so-called PD which can be checked out mentioned later) of a portable device (Portable Device (it is also called PD)) which can use the contents corresponding to the data of the use condition for coincidence, for example. Even when only the number shown in the data of use conditions checks out contents, a personal computer 1 can reproduce the contents.
[0005] The display operator guidance program 11 of a personal computer 1 inputs directions of check-out etc., and makes LCM (Licensed Compliant Module)12 which is a software module based on the specification of SDMI (Secure Digital Music Initiative) perform processing of the check-out corresponding to the directions etc. while it displays the data (for example, a music name or use conditions etc.) relevant to the contents which the personal computer 1 is recording.
[0006] LCM12 of a personal computer 1 consists of module groups which control to be able to use contents only on the use conditions which a copyright person specifies to each contents for the purpose of prevention of infringement of the copyright by unjust secondary use of contents. Playback conditions, copy conditions, migration conditions, or are recording conditions of contents etc. are included in use conditions.
[0007] LCM12 attests whether the device connected to the personal computer 1 is just, and performs processing of migration of contents etc. by the safe approach. With processing of migration of contents etc., LCM12 generates a required key, manages a key, enciphers contents or controls the communication link with the device connected.
[0008] Moreover, LCM12 checks the justification of the portable media 3 with which it is equipped, adds the use conditions specified by a server 5 to contents (enciphered), and makes contents record.
[0009] LCM12 of a personal computer 1 updates the data of the use conditions corresponding to the contents which supplied them corresponding to having supplied the portable device 2 with the data (for example, a music name or use conditions etc.) relevant to contents while supplying the contents currently enciphered and recorded to the portable device 2 connected (check-out is called hereafter). The count which can check out the data of the use conditions corresponding to the contents which the personal computer 1 is recording on it more when you check out in a detail is reduced by one. Corresponding contents cannot be checked out when the count which can be checked out is 0.
[0010] The portable device 2 makes the portable media 3 with which it is equipped with the data (for example, a music name or use conditions etc.) relevant to contents memorize the contents (namely, checked-out contents) supplied from the personal computer 1.
[0011] The portable media 3 have storages, such as a flash memory, in the interior, and are constituted by the portable device 2 removable.

[0012] Based on the data of the use conditions relevant to contents, the portable device 2 is reproduced and outputs the contents memorized by the portable media 3 with which it is equipped to the headphone which are not illustrated.
[0013] For example, when it is going to reproduce exceeding the count of playback as a playback limit memorized as data of the use conditions relevant to contents, the portable device 2 suspends playback of corresponding contents.
[0014] A user can remove and walk around with the portable device 2 which memorized contents from a personal computer 1, can reproduce the contents memorized by the portable media 3, and can listen to the music corresponding to contents etc. by headphone etc.
[0015] When the portable device 2 is connected to a personal computer 1 through a USB cable etc., the portable device 2 and a personal computer 1 perform processing of mutual recognition. Processing of this mutual recognition is processing of authentication of a challenge response method. A challenge response method is a method which answers with the value (response) which the portable device 2 generated to a certain value (challenge) which a personal computer 1 generates using the private key currently shared with a personal computer 1.
[0016] A server 5-1 distributes the contents which compression coding is carried out by the predetermined method, accumulate the enciphered contents, and are accumulated corresponding to the demand from a personal computer 1. A server 5-1 has the function of the key server 21-1, the contents server 22-1, and the shop server 23-1.
[0017] The key server 21-1 accumulates the contents key for decoding the contents which the contents server 22-1 supplied to the personal computer 1, and supplies a contents key to a personal computer 1 corresponding to the demand of a personal computer 1. Before supply of a contents key, the key server 21-1 and a personal computer 1 perform processing of mutual recognition, and the key server 21-1 enciphers a contents key with a key temporarily which was shared by processing of the mutual recognition, and transmits them to a personal computer 1. A personal computer 1 is decoded with a key temporarily which is sharing the received contents key.
[0018] The contents server 22-1 supplies contents (enciphered) to a personal computer 1 with the use conditions corresponding to contents through a communication network 4 corresponding to the demand of a personal computer 1.
[0019] While the shop server 23-1 provides a personal computer 1 with the digital data (the list of the contents containing the music name of contents, a price, etc. is included) relevant to the contents which the contents server 22-1 supplies It corresponds to the application of the purchase of the contents from a personal computer 1. URL (Uniform Resource Locator) of the contents server 22-1 which supplies the contents, URL of the key server 21-1 which supplies the contents key which decodes the contents, etc. are supplied to a personal computer 1.
[0020] A server 5-2 distributes the contents which compression coding is carried out by the predetermined method, accumulate the enciphered contents, and are accumulated corresponding to the demand from a personal computer 1. A server 5-2 has the function of the key server 21-2, the contents server 22-2, and the shop server 23-2.
[0021] The key server 21-2 accumulates the contents key for decoding the contents which the contents server 22-2 supplied to the personal computer 1, and supplies a contents key to a personal computer 1 corresponding to the demand of a personal

computer 1. Before supply of a contents key, the key server 21-2 and a personal computer 1 perform processing of mutual recognition, and the key server 21-2 enciphers a contents key with a key temporarily which was shared by processing of the mutual recognition, and transmits them to a personal computer 1. A personal computer 1 is decoded with a key temporarily which is sharing the received contents key.
[0022] The contents server 22-2 supplies contents (enciphered) to a personal computer 1 with the use conditions corresponding to contents through a communication network 4 corresponding to the demand of a personal computer 1.
[0023] While the shop server 23-2 provides a personal computer 1 with the digital data (the list of the contents containing the music name of contents, a price, etc. is included) relevant to the contents which the contents server 22-2 supplies It corresponds to the application of the purchase of the contents from a personal computer 1. URL of the contents server 22-2 which supplies the contents, URL of the key server 21-2 which supplies the contents key which decodes the contents, etc. are supplied to a personal computer 1.
[0024] Hereafter, when it is not necessary to distinguish a server 5-1 and a server 5-2 separately, a server 5 is only called. Hereafter, when it is not necessary to distinguish the key server 21-1 and the key server 21-2 separately, the key server 21 is only called. Hereafter, when it is not necessary to distinguish the contents server 22-1 and the contents server 22-2 separately, the contents server 22 is only called. Hereafter, when it is not necessary to distinguish the shop server 23-1 and the shop server 23-2 separately, the shop server 23 is only called.
[0025] Next, with reference to drawing 2 , the configuration of the function of the conventional digital data transmission system is explained. In addition to the display operator guidance program 11 and LCM12, a personal computer 1 performs the IP (Internet Protocol) communications program 13, the ISP (Internet Service Provider) connection program 14, and the PHS (Personal Handyphone System) / IMT (International Mobile Telecommunication System) communications program 15.
[0026] The PHS/IMT communications program 15 is a program for communicating through the public line network 31. The ISP connection program 14 is a program for connecting with ISP32. The IP communications program 13 is a program for including procedures, such as HTTP (Hypertext Transport Protocol)74 and Wap (Wireless Access Protocol)75, and communicating with the key server 21, the contents server 22, or the shop server 23 through a communication network 4.
[0027] LCM12 consists of the license manager 51, a download program 52-1, a download program 52-2, and a format manager 53.
[0028] The license manager 51 is a program for managing the use of contents based on the use conditions of contents, and consists of a use condition manager 61, a CD ripping program 62, and a PD authentication program 63.
[0029] The use condition manager 61 updates the data of use conditions corresponding to check-out of contents etc. while performing management of whether check-out of the contents which the personal computer 1 is recording etc. is permitted based on the use conditions of contents, or to forbid. CD ripping program 62 generates the use conditions corresponding to the read contents while reading contents from CD with which the personal computer 1 was equipped.

[0030] PD authentication program 63 attests the portable device 2 with which the personal computer 1 is equipped.
[0031] The download program 52-1 is a program for downloading contents and a contents key from a server 5-1, and consists of the key manager 64, a contents manager 65, a key information receiving agent 66, and a contents information receiving agent 67.
[0032] The key manager 64 performs processing of authentication of the key server 21-1, receives a contents key from the key server 21-1, is made to run on contents, and manages a contents key. The key manager 64 consists of a server authentication program 71 and a receiving agent 72.
[0033] The server authentication program 71 attests the key server 21-1 by processing mentioned later. A receiving agent 72 receives a contents key from the key server 21-1 through a communication network 4.
[0034] Through a communication network 4, the contents manager 65 receives contents with the data of the use conditions of contents from the contents server 22-1, and records contents with the data of the use conditions of contents. The receiving agent 73 of the contents manager 65 receives the data and contents of use conditions of contents from the contents server 22-1.
[0035] The key information receiving agent 66 receives URL which specifies the key server 21-1 which supplies the contents key corresponding to desired contents from the shop server 23-1. The contents information receiving agent 67 receives URL which specifies the content ID which specifies the contents for which a user asks from the shop server 23-1, and the contents server 22-1 which supplies the contents.
[0036] The download program 52-2 is a program for downloading contents and a contents key from a server 5-2, and since it has the same configuration as the download program 52-1, it omits the explanation.
[0037] The format manager 53 encodes the contents read from CD by the predetermined method, and enciphers while it transforms into a predetermined method the coding method and cipher system of contents which were downloaded from the contents server 22-1 or 22-2, respectively. The format manager 53 consists of a system discernment program 68 and a format conversion program 69.
[0038] The system discernment program 68 is a program for the download place of contents to identify whether it is a server 5-1 or it is a server 5-2. The format conversion program 69 changes the coding method and cipher system of contents.
[0039] The portable device 2 performs the license manager 81, the key manager 82, and the contents manager 83.
[0040] The license manager 81 consists of a use condition manager 91 which manages the count of playback of contents etc. based on the use conditions corresponding to contents, a PC authentication program 92 which attests a personal computer 1, and a PM authentication program 93 which attests the portable media 3.
[0041] Make it encipher with the key for preservation with which the portable media 3 have memorized beforehand the contents key supplied from the personal computer 1, and the portable media 3 are made to memorize the key manager 82, and it is managed.
[0042] The contents manager 83 makes the portable media 3 memorize the contents supplied from the personal computer 1, and manages them.

[0043] The portable media 3 perform the license manager 101, the key manager 102, and the contents manager 103.
[0044] The license manager 101 has PD authentication program 111 which attests the portable device 2, memorizes the data of the use conditions corresponding to contents, and controls read-out of contents etc. based on the data of use conditions. The key manager 102 enciphers, memorizes and manages the contents key supplied from the portable device 2 with the key for preservation memorized beforehand. The contents manager 103 memorizes and manages the contents supplied from the portable device 2.
[0045] The shop server 23-1 performs the key information transmitting program 121, the contents information transmitting program 122, the perusal program 123, and the IP communications program 124.
[0046] The key information transmitting program 121 transmits URL of the key server 21-1 which supplies the contents key corresponding to the contents for which the user of a personal computer 1 asks in a personal computer 1 through a communication network 4.
[0047] The contents information transmitting program 122 transmits URL of the contents server 22-1 which supplies the contents for which the user of a personal computer 1 asks in a personal computer 1 through a communication network 4.
[0048] The perusal program 123 consists of a viewing-and-listening program 131 which makes the user of a personal computer 1 view and listen to contents, and a retrieval program 132 whose user of a personal computer 1 searches desired contents.
[0049] The IP communications program 124 is a program for including procedures, such as HTTP133 and Wap134, and communicating with a personal computer 1 through a communication network 4.
[0050] The key server 21-1 performs the authentication program 151, the key distribution program 152, the key preservation program 153, the key generator 154, and the IP communications program 155.
[0051] The authentication program 151 is a program which attests a personal computer 1 etc. The key distribution program 152 is a program which distributes the contents key which the key preservation program 153 saves in the attested personal computer 1. The key preservation program 153 is a program which saves the contents key generated by the key generator 154. The key generator 154 is a program which is made to run on contents and generates a contents key.
[0052] The IP communications program 155 is a program for including procedures, such as HTTP171 and Wap172, and communicating with a personal computer 1 etc. through a communication network 4.
[0053] The contents server 22-1 performs the contents preservation program 191, the contents distribution program 192, and the IP communications program 193.
[0054] The contents preservation program 191 makes the contents enciphered correspond with content ID, and saves them. The contents distribution program 192 distributes the contents corresponding to content ID which the contents preservation program 191 saves to a personal computer 1, when there is a demand from a personal computer 1.
[0055] The IP communications program 193 is a program for including procedures, such as HTTP201 and Wap202, and communicating with a personal computer 1 through a communication network 4.

[0056] Since it has the same configuration as the shop server 23-1, the shop server 23-2 omits the explanation. Since it has the same configuration as the key server 21-1, the key server 21-2 omits the explanation. Since it has the same configuration as the contents server 22-1, the contents server 22-2 omits the explanation.
[0057] Next, a personal computer 1 downloads contents from a server 5-1, and the conventional processing which he checks out to the portable device 2 is explained with reference to the flow chart of drawing 3 and drawing 4 . In step S101, PHS / IMT communications program 15 of a personal computer 1 establish the public line network 31 and connection. In step S201, the earth station which the public line network 31 does not illustrate establishes a personal computer 1 and connection.
[0058] In step S102, the ISP connection program 14 of a personal computer 1 establishes ISP32 and connection. In step S301, ISP32 establishes a personal computer 1 and connection.
[0059] In step S103, the IP communications program 13 of a personal computer 1 establishes the shop server 23 and IP communication link. In step S401, the IP communications program 124 of the shop server 23-1 establishes a personal computer 1 and IP communication link.
[0060] In step S402, the perusal program 123 of the shop server 23-1 transmits the digital data for perusal (for selection of contents) to a personal computer 1 through a communication network 4. The browser program which a personal computer 1 does not illustrate displays an image or a text corresponding to digital data etc., and a user is made to peruse it in step S104. Moreover, the browser program of a personal computer 1 makes a user try listening contents by streaming playback of contents, or makes the perusal program 123 of the shop server 23-1 search contents by the keyword, and displays the result. Processing of step S402 and step S104 is repeated corresponding to a demand of the user of a personal computer 1.
[0061] In step S105, the browser program of a personal computer 1 transmits a purchase request to the shop server 23-1. In step S403, the perusal program 123 of the shop server 23-1 receives the purchase request transmitted from the personal computer 1.
[0062] In step S404, the contents information transmitting program 122 of the shop server 23-1 transmits the contents information containing the content ID for specifying URL and contents of the contents server 22-1 which distribute the contents corresponding to the purchase request which received by processing of step S403 etc. to a personal computer 1 through a communication network 4. In step S106, the contents information receiving agent 67 of a personal computer 1 receives the contents information which the shop server 23-1 transmitted.
[0063] In step S405, the key information transmitting program 121 of the shop server 23-1 transmits key information, such as URL of the key server 21-1 which distributes the contents key of the contents corresponding to the purchase request which received by processing of step S403, to a personal computer 1 through a communication network 4. In step S107, the key information receiving agent 66 of a personal computer 1 receives the key information which the shop server 23-1 transmitted.
[0064] In step S108, the IP communications program 13 of a personal computer 1 establishes the contents server 22-1 and IP communication link based on URL of the contents server 22-1 contained in the contents information acquired by processing of

step S106. In step S501, the IP communications program 193 of the contents server 22-1 establishes a personal computer 1 and IP communication link.
[0065] In step S109, the contents manager 65 of a personal computer 1 transmits the content ID acquired by processing of step S106 to the contents server 22-1 through a communication network 4. In step S502, the contents server 22-1 receives the content ID which the personal computer 1 transmitted. In step S503, the contents distribution program 192 of the contents server 22-1 reads the contents (enciphered) corresponding to the content ID which received at step S502 from the contents preservation program 191, and distributes them to a personal computer 1 through a communication network 4. In step S110, the receiving agent 73 of the contents manager 65 of a personal computer 1 receives the contents which the contents server 22-1 transmitted.
[0066] In step S111, the IP communications program 13 of a personal computer 1 establishes the key server 21-1 and IP communication link based on URL of the key server 21-1 contained in the key information acquired by processing of step S107. In step S601, the IP communications program 155 of the key server 21-1 establishes a personal computer 1 and IP communication link.
[0067] In step S112, the server authentication program 71 of the key manager 64 of a personal computer 1 attests the key server 21-1. In step S602, the authentication program 151 of the key server 21-1 attests a personal computer 1.
[0068] The master key KMS is beforehand memorized by the key server 21-1, and ID of the individual key KPP and a personal computer 1 is beforehand memorized by the personal computer 1. The master key KMP is further memorized beforehand by the personal computer 1, and ID and the individual key KPS of the key server 21-1 are memorized by the key server 21-1.
[0069] The key server 21-1 receives supply of ID of a personal computer 1 to the personal computer 1, applies a Hash Function to the master key KMS which the ID and themselves have, and generates the same key as the individual key KPP of a personal computer 1.
[0070] A personal computer 1 receives supply of ID of the key server 21-1 to the key server 21-1, applies a Hash Function to the master key KMP which the ID and themselves have, and generates the same key as the individual key KPS of the key server 21-1. A personal computer 1 and an individual key common to both key servers 21-1 will be shared between doing in this way. A key is further generated temporarily using these individual keys.
[0071] In step S113, the key manager 64 of a personal computer 1 transmits content ID to the key server 21-1. In step S603, the key server 21-1 receives the content ID which the personal computer 1 transmitted. In step S604, the key distribution program 152 of the key server 21-1 reads the contents key which the key preservation program 153 matches with content ID, and is saved, and transmits the contents key (enciphered with the key temporarily) to a personal computer 1 through a communication network 4. In step S114, the receiving agent 72 of the key manager 64 of a personal computer 1 receives the contents key which the key server 21-1 transmitted. The key manager 64 decodes the received contents key with a key temporarily.
[0072] In step S115, the PHS/IMT communications program 15 of a personal computer 1 cuts connection with the public line network 31. In step S202, the earth station which the public line network 31 does not illustrate cuts connection with a personal computer 1.

[0073] In step S116, the format manager 53 transforms into a predetermined method the coding method and cipher system of contents which were received by processing of step S110, respectively.
[0074] When the user of a personal computer 1 directs check-out of the contents which received to the display operator guidance program 11, processing after step S117 is performed.
[0075] In step S117, PD authentication program 63 of the license manager 51 of a personal computer 1 attests the portable device 2. In step S701, PC authentication program 92 of the license manager 81 of the portable device 2 attests a personal computer 1.
[0076] Processing of the mutual recognition of the personal computer 1 and the portable device 2 in step S117 and step S701 is processing of authentication of a challenge response method, and there are few amounts of operations as compared with processing of the mutual recognition of the key server 21-1 and personal computer 1 in step S112 and step S602. A personal computer 1 and the portable device 2 are the same operations, and generate and share a key from a response temporarily, respectively.
[0077] In step S118, the contents manager 65 of a personal computer 1 distributes the contents enciphered to the portable device 2. In step S702, the contents manager 83 of the portable device 2 receives the contents which the personal computer 1 distributed, and supplies them to the contents manager 103 of the portable media 3. The contents manager 103 of the portable media 3 memorizes contents.
[0078] In addition, when the portable device 2 is equipped with the portable media 3, mutual recognition of the portable device 2 and the portable media 3 is carried out.
[0079] In step S119, the key manager 64 of a personal computer 1 distributes the contents key (enciphered with the key temporarily which is shared between the portable device 2 and the portable media 3) corresponding to the contents distributed to the portable device 2 at step S118. In step S703, the key manager 82 of the portable device 2 receives the contents key which the personal computer 1 distributed, and supplies it to the key manager 102 of the portable media 3. The key manager 102 of the portable media 3 decodes a contents key with a key temporarily, and memorizes a contents key.
[0080] Next, a personal computer 1 downloads contents from a server 5-2, and the processing which he checks out to the portable device 2 is explained with reference to the flow chart of drawing 5 and drawing 6 . Processing of step S1101 thru/or step S1107 is performed by a server 5-2 and the list by the IP communications program 13, the ISP connection program 14, the PHS/IMT communications program 15, and the download program 52-2, and since it is the same as that of processing of step S101 thru/or step S107, the explanation is omitted, respectively.
[0081] In step S1108, the IP communications program 13 of a personal computer 1 establishes the key server 21-2 and IP communication link based on URL of the key server 21-2 contained in the key information acquired by processing of step S1107. In step S1601, the key server 21-2 establishes a personal computer 1 and IP communication link.
[0082] In step S1109, the download program 52-2 of a personal computer 1 attests the key server 21-2. In step S1602, the key server 21-2 attests a personal computer 1.

Processing of step S1109 and step S1602 is the same processing as processing of step S112 and step S602.
[0083] In step S1110, the download program 52-2 of a personal computer 1 transmits content ID to the key server 21-2. In step S1603, the key server 21-2 receives the content ID which the personal computer 1 transmitted. In step S1604, the key server 21-2 reads the contents key which matches with content ID and is saved, and transmits the contents key (enciphered with the key temporarily) to a personal computer 1 through a communication network 4. In step S1111, the download program 52-2 of a personal computer 1 receives the contents key which the key server 21-2 transmitted. The download program 52-2 decodes the received contents key with a key temporarily.
[0084] Step S1112 Setting, the IP communications program 13 of a personal computer 1 establishes the contents server 22-2 and IP communication link based on URL of the contents server 22-2 contained in the contents information acquired by processing of step S1106. In step S1501, the contents server 22-2 establishes a personal computer 1 and IP communication link.
[0085] In step S1113, the download program 52-2 of a personal computer 1 transmits the content ID acquired by processing of step S1106 to the contents server 22-2 through a communication network 4. In step S1502, the contents server 22-2 receives the content ID which the personal computer 1 transmitted. In step S1503, the contents server 22-2 reads the contents (enciphered) corresponding to the content ID which received at step S1502, and distributes them to a personal computer 1 through a communication network 4. In step S1114, the download program 52-2 of a personal computer 1 receives the contents which the contents server 22-2 transmitted.
[0086] Since processing of step S1115 thru/or step S1703 is the same as processing of step S115 thru/or step S703, the explanation is omitted.
[0087]
[Problem(s) to be Solved by the Invention] As mentioned above, since the procedures which supply contents and a contents key differ, respectively, when the server 5-1 which supplies contents and a contents key, or 5-2 asks for reception of a server 5-1 and the contents from 5-2, the download program 52-1 corresponding to a server 5-1 and the download program 52-2 corresponding to a server 5-2 are needed.
[0088] However, when a throughput, like there is little storage capacity with the small arithmetic proficiency of the equipment which receives contents is small, the equipment which receives contents cannot memorize two or more download programs, cannot switch a download program and cannot perform them.
[0089] This invention is made in view of such a situation, and it aims at enabling it to receive the contents and the key which are supplied in the procedure in which throughputs differ also with small equipment.
[0090]
[Means for Solving the Problem] 1st authentication means by which information offer equipment according to claim 1 attests the 1st information processor, The 2nd authentication means which attests the 2nd information processor or 3rd information processor, A reception-control means to control the reception of data which specifies the data which specify the 2nd information processor as the Request to Send of the contents and the key from the 1st information processor, and a list, or the 3rd information processor, When the data which specify the 2nd information processor are

received, in the procedure corresponding to the 2nd information processor While transmitting the Request to Send of contents and a key to the 2nd information processor When contents and a key are received from the 2nd information processor and the data which specify the 3rd information processor are received, in the procedure corresponding to the 3rd information processor While transmitting the Request to Send of contents and a key to the 3rd information processor It is characterized by including a communications control means to control a communication link to receive contents and a key from the 3rd information processor, and a transmission-control means to control the contents to the 1st information processor, and transmission of a key.
[0091] Information offer equipment establishes further a conversion means to transform either [ at least ] the coding method of contents, or the cipher systems into a predetermined coding method or a predetermined cipher system, and is made in things.
[0092] The 1st authentication step with which the information offer approach according to claim 3 attests the 1st information processor, The 2nd authentication step which attests the 2nd information processor or 3rd information processor, The reception-control step which controls the reception of data which specifies the data which specify the 2nd information processor as the Request to Send of the contents and the key from the 1st information processor, and a list, or the 3rd information processor, When the data which specify the 2nd information processor are received, in the procedure corresponding to the 2nd information processor While transmitting the Request to Send of contents and a key to the 2nd information processor When contents and a key are received from the 2nd information processor and the data which specify the 3rd information processor are received, in the procedure corresponding to the 3rd information processor While transmitting the Request to Send of contents and a key to the 3rd information processor It is characterized by including the communications control step which controls a communication link to receive contents and a key from the 3rd information processor, and the transmission-control step which controls the contents to the 1st information processor, and transmission of a key.
[0093] The program of a program storing medium according to claim 4 The 1st authentication step which attests the 1st information processor, and the 2nd authentication step which attests the 2nd information processor or 3rd information processor, The reception-control step which controls the reception of data which specifies the data which specify the 2nd information processor as the Request to Send of the contents and the key from the 1st information processor, and a list, or the 3rd information processor, When the data which specify the 2nd information processor are received, in the procedure corresponding to the 2nd information processor While transmitting the Request to Send of contents and a key to the 2nd information processor When contents and a key are received from the 2nd information processor and the data which specify the 3rd information processor are received, in the procedure corresponding to the 3rd information processor While transmitting the Request to Send of contents and a key to the 3rd information processor It is characterized by including the communications control step which controls a communication link to receive contents and a key from the 3rd information processor, and the transmission-control step which controls the contents to the 1st information processor, and transmission of a key.

[0094] An authentication means by which an information processor according to claim 5 attests the 1st information offer equipment, The contents to the 1st information offer equipment and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with contents and a key, And a transmission-control means to control transmission of either of the data which specifies the 3rd information offer equipment which offers contents and a key, It is characterized by including a reception-control means for the 1st information offer equipment to receive offer from the 2nd information offer equipment or the 3rd information offer equipment, and to control reception of the contents and the key which were transmitted.
[0095] The authentication step with which the information processing approach according to claim 6 attests the 1st information offer equipment, The contents to the 1st information offer equipment and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with contents and a key, And the transmission-control step which controls transmission of either of the data which specifies the 3rd information offer equipment which offers contents and a key, It is characterized by including the reception-control step which the 1st information offer equipment receives offer from the 2nd information offer equipment or the 3rd information offer equipment, and controls reception of the contents and the key which were transmitted.
[0096] The program of a program storing medium according to claim 7 The authentication step which attests the 1st information offer equipment, and the 1st information offer equipment, Contents and the Request to Send of a key, the data that specify the 2nd information offer equipment which provides a list with contents and a key, And the transmission-control step which controls transmission of either of the data which specifies the 3rd information offer equipment which offers contents and a key, It is characterized by including the reception-control step which the 1st information offer equipment receives offer from the 2nd information offer equipment or the 3rd information offer equipment, and controls reception of the contents and the key which were transmitted.
[0097] In information offer equipment according to claim 1, the information offer approach according to claim 3, and a program storing medium according to claim 4 The 1st information processor is attested and the 2nd information processor or 3rd information processor is attested. The reception of data which specifies the data which specify the 2nd information processor as the Request to Send of the contents and the key from the 1st information processor and a list, or the 3rd information processor is controlled. When the data which specify the 2nd information processor are received, in the procedure corresponding to the 2nd information processor While transmitting the Request to Send of contents and a key to the 2nd information processor When contents and a key are received from the 2nd information processor and the data which specify the 3rd information processor are received, in the procedure corresponding to the 3rd information processor While transmitting the Request to Send of contents and a key to the 3rd information processor, a communication link is controlled to receive contents and a key from the 3rd information processor, and the contents to the 1st information processor and transmission of a key are controlled.
[0098] In an information processor according to claim 5, the information processing approach according to claim 6, and a program storing medium according to claim 7 The

1st information offer equipment is attested. The contents to the 1st information offer equipment, and the Request to Send of a key, The data which specify the 2nd information offer equipment which provides a list with contents and a key, And transmission of either of the data which specifies the 3rd information offer equipment which offers contents and a key is controlled, the 1st information offer equipment receives offer from the 2nd information offer equipment or the 3rd information offer equipment, and reception of the contents and the key which were transmitted is controlled.

[0099]

[Embodiment of the Invention] Drawing 7 is drawing showing the gestalt of 1 operation of the digital data transmission system concerning this invention. The same number as the case of drawing 1 is given to the same part as the case of a configuration of that drawing 1 explained, and the explanation is omitted.

[0100] The portable media 3-1 are constituted possible [ wearing ], and the telephone one apparatus terminal 501 is connected to a communication network 4 by wireless. The telephone one apparatus terminal 501 downloads the contents (compressed and enciphered by the predetermined method) which received from the contents server 22-1 or 22-2 with the data of use conditions etc. through a communication network 4, and the portable media 3-1 equipped with contents and its use condition data are made to memorize it.

[0101] Based on the data of the use conditions relevant to contents, the telephone one apparatus terminal 501 is reproduced and outputs the contents memorized by the portable media 3-1 with which it is equipped to headphone or a loudspeaker etc. which is not illustrated. Walking around with the telephone one apparatus terminal 501, a user can download desired contents in a desired location, and can make the portable media 3-1 memorize the contents. A user can make the telephone one apparatus terminal 501 able to reproduce the contents memorized by the portable media 3-1, and can listen to the music corresponding to contents etc. by headphone etc.

[0102] The display operator guidance program 511 of the telephone one apparatus terminal 501 inputs directions of download etc., and makes LCM512 for clients perform processing corresponding to the directions while it displays the data (for example, a music name or use conditions etc.) relevant to contents. LCM512 for clients of the telephone one apparatus terminal 501 performs a series of processings (it mentions later) which download use condition data, contents, etc. in cooperation with LCM514 for servers of the substitute server 503.

[0103] LCM512 for clients of the telephone one apparatus terminal 501 consists of module groups which control to be able to use contents only on the use conditions which a copyright person specifies to each contents for the purpose of prevention of infringement of the copyright by unjust secondary use of contents. Playback conditions, copy conditions, migration conditions, or are recording conditions of contents etc. are included in use conditions.

[0104] LCM512 for clients attests whether the portable media 3-1 with which the telephone one apparatus terminal 501 is equipped are just, adds the data of the use conditions which the server 5 specified by the safe approach to contents (enciphered), and makes contents record on the portable media 3-1. With processing of migration of

contents etc., LCM512 for clients generates a required key, manages a key or controls the communication link with the portable media 3-1 connected.
[0105] The personal computer 502 is connected to the communication network 4. With cipher systems, such as DES, it enciphers and a personal computer 502 records them while changing into the method of predetermined compression the contents which received from the contents server 22-1 or 22-2, or were read in CD. A personal computer 502 records the data of use conditions in which the use conditions of contents are shown corresponding to the contents currently enciphered and recorded.
[0106] The display operator guidance program 11 of a personal computer 502 inputs directions of download or check-out etc., and makes LCM513 perform processing of the download corresponding to the directions, or check-out while it displays the data (for example, a music name or use conditions etc.) relevant to contents.
[0107] LCM513 of a personal computer 502 consists of module groups which control to be able to use contents only on the use conditions which a copyright person specifies to each contents for the purpose of prevention of infringement of the copyright by unjust secondary use of contents. Playback conditions, copy conditions, migration conditions, or are recording conditions of contents etc. are included in use conditions.
[0108] LCM513 attests whether the portable device 2 connected to the personal computer 502 is just, and performs processing of migration of contents etc. by the safe approach. With processing of migration of contents etc., LCM513 generates a required key, manages a key, enciphers contents or controls the communication link with the device connected.
[0109] Moreover, LCM513 checks the justification of the portable device 2. The portable device 2 checks the justification of the portable media 3-2, when equipped with the portable media 3-2. When the portable device 2 and the portable media 3-2 are just, LCM513 adds the data of the use conditions specified by a server 5 to contents (enciphered), and checks out contents to the portable media 3-2. The portable device 2 makes the portable media 3-2 with which it is equipped with the data relevant to contents memorize the contents by which the personal computer 502 was checked out.
[0110] LCM513 of a personal computer 502 checks out the contents currently enciphered and recorded to the portable device 2 connected. The portable device 2 makes the portable media 3-2 with which it is equipped with the data relevant to contents memorize the contents by which the personal computer 502 was checked out.
[0111] When the substitute server 503 can be used, LCM521 (it consists of the part or all the functions of LCM513) for PC of a personal computer 502 performs a series of processings which download use condition data, contents, etc. in cooperation with LCM514 for servers of the substitute server 503.
[0112] When the substitute server 503 cannot be used, LCM513 of a personal computer 502 performs processing of authentication with the same key server 21-1 or 21-2 [ same ] as LCM12 etc., and downloads use condition data, contents, etc.
[0113] The substitute server 503 performs processing of authentication with the key server 21-1 or 21-2 corresponding to the demand of the telephone one apparatus terminal 501 which performed and carried out mutual recognition of LCM514 for servers, or the personal computer 502 which carried out mutual recognition. The substitute server 503 supplies the contents key which received the contents key and was received from the key server 21-1 or 21-2 to the telephone one apparatus terminal 501 or a

personal computer 502 after processing of the key server 21-1 or the mutual recognition of 21-2. The substitute server 503 supplies the contents which received contents and received from the contents server 22-1 or 22-2 to the telephone one apparatus terminal 501 or a personal computer 502.
[0114] The substitute server 503 receives a contents key, after receiving contents from a server 5-1, when downloading contents and a contents key from a server 5-1. The substitute server 503 receives contents, after receiving a contents key, when downloading contents and a contents key from a server 5-2.
[0115] In any case, it is the same procedure (for example, contents are transmitted after transmitting a contents key), and the substitute server 503 supplies contents and a contents key for it to the telephone one apparatus terminal 501 or a personal computer 502, also when contents and a contents key are downloaded from a server 5-1, and also when contents and a contents key are downloaded from a server 5-2.
[0116] The telephone one apparatus terminal 501 or a personal computer 502 can receive contents and a contents key in the same procedure through the substitute server 503 by downloading contents and a contents key from a server 5-1 or 5-2.
[0117] Drawing 8 is drawing explaining the configuration of the telephone one apparatus terminal 501. CPU (CentralProcessing Unit)601 actually performs the various programs stored in ROM (Read-only Memory)602 or RAM (Random-Access Memory)603. ROM602 consists of an EEPROM (Electrically Erasable Programmable Read-Only Memory) or a flash memory, and, generally stores the data of immobilization fundamentally of the parameters the program which CPU601 uses, and for an operation. RAM603 consists of SRAM (Static RAM) etc., and stores a variable parameter suitably in the program used in activation of CPU601, and its activation.
[0118] The input section 605 is operated by the user, when it consists of an input key or a microphone and various kinds of commands are inputted into CPU601, or when inputting voice etc. A display 606 consists of a liquid crystal display etc., and displays various information in a text or an image.
[0119] The voice playback section 607 reproduces the contents memorized by the portable media 3-1 supplied from the data of a message partner's voice supplied from the communications department 608, or an interface 609, and outputs voice.
[0120] The communications department 608 connects with the public line network 31, stores in the packet of a predetermined method the data of a user's voice supplied from the data (for example, Request to Send of contents etc.) or the input section 605 supplied from CPU601, and transmits through the public line network 31. Moreover, the communications department 608 outputs the data (for example, contents etc.) stored in the packet which received, or the data of a message partner's voice to CPU601, RAM603, the voice playback section 607, or an interface 609 through the public line network 31.
[0121] It reads data, such as contents, from the portable media 3-1 with which it is equipped, and supplies them to CPU601, RAM603, or the voice playback section 607 while making the portable media 3-1 equipped with CPU601, RAM603, or the data supplied from the communications department 608 memorize an interface 609.
[0122] As for an interface 610, the external drive 631 is connected. Drive 631 reads the data or the program currently recorded on the magnetic disk 641 with which it is equipped, an optical disk 642 (CD-ROM is included), a magneto-optic disk 643, or

semiconductor memory 644, and supplies the data or program to ROM602 or RAM603 which are connected through the interface 610 and the bus 604.
[0123] CPU601 thru/or the interface 610 are mutually connected by the bus 604.
[0124] Drawing 9 is drawing explaining the configuration of the substitute server 503. CPU651 actually performs various application programs (for details, it mentions later) and OS (Operating System). Generally ROM652 stores the data of immobilization fundamentally of the parameters the program which CPU651 uses, and for an operation. RAM653 stores a variable parameter suitably in the program used in activation of CPU651, and its activation. These are mutually connected by the host bus 654 which consists of CPU buses etc.
[0125] The host bus 654 is connected to the external buses 656, such as a PCI (Peripheral Component Interconnect/Interface) bus, through the bridge 655.
[0126] A keyboard 658 is operated by the user when inputting various kinds of commands into CPU651. A pointing device 659 is operated by the user when performing the directions and selection of the point on the screen of a display 660. A display 660 consists of a liquid crystal display or CRT (Cathode Ray Tube), and displays various information in a text or an image. HDD (Hard Disk Drive)661 drives a hard disk, and records or reproduces the program and information which are performed by CPU651 to them.
[0127] Drive 662 reads the data or the program currently recorded on the magnetic disk 681 with which it is equipped, an optical disk 682, a magneto-optic disk 683, or semiconductor memory 684, and supplies the data or program to RAM653 with which it connects through the interface 657, the external bus 656, the bridge 655, and the host bus 654.
[0128] These keyboards 658 thru/or drives 662 is connected to the interface 657, and the interface 657 is connected to CPU651 through the external bus 656, the bridge 655, and the host bus 654.
[0129] The communications department 663 outputs the data (for example, content ID etc.) stored in the packet which received to CPU651, RAM653, or HDD661 through a communication network 4 while a communication network 4 is connected, and it stores in the packet of a predetermined method the data (for example, contents key etc.) supplied from CPU651 or HDD661 and transmits through a communication network 4.
[0130] The communications department 663 is connected to CPU651 through the external bus 656, the bridge 655, and the host bus 654.
[0131] Next, with reference to drawing 10 , the configuration of the function of the digital data transmission system of this application is explained. The same number as the case of drawing 2 is given to the same part as the case of a configuration of that drawing 2 explained, and the explanation is omitted.
[0132] The telephone one apparatus terminal 501 performs the display operator guidance program 511, LCM512 for clients, the IP communications program 701, the ISP connection program 702, and the PHS/IMT communications program 703.
[0133] The PHS/IMT communications program 703 is a program for communicating through the public line network 31. The ISP connection program 702 is a program for connecting with ISP32. The IP communications program 701 is a program for including procedures, such as HTTP741 and Wap742, and communicating with the key server 21-1, the contents server 22-1, the shop server 23-1, the key server 21-2, the contents

server 22-2, the shop server 23-2, or the substitute server 503 through a communication network 4.
[0134] LCM512 for clients consists of a license manager 711, a download program 712, a format manager 713, etc.
[0135] The license manager 711 is a program for managing the use of contents based on the use conditions of contents, and consists of a use condition manager 721, a server authentication program 722, a PM authentication program 723, etc.
[0136] The use condition manager 721 makes the data of the use conditions which the portable media 3-1 have memorized to the portable media 3-1 update corresponding to playback of the contents which the portable media 3-1 have memorized etc. while performing management of whether playback of the contents which the portable media 3-1 have memorized etc. is permitted based on the use conditions of contents, or to forbid. The server authentication program 722 attests the substitute server 503 through a communication network 4. PM authentication program 723 attests the portable media 3-1, when the telephone one apparatus terminal 501 is equipped with the portable media 3-1.
[0137] The download program 712 consists of the key manager 724, a contents manager 725, a key information receiving agent 726, a contents information receiving agent 727, etc.
[0138] The key manager 724 receives a contents key from the substitute server 503, is made to run on contents, makes the portable media 3-1 memorize a contents key, and manages it. The key manager 724 contains the receiving agent 731 which receives a contents key from the substitute server 503.
[0139] The contents manager 725 receives contents (enciphered) with the use conditions of contents from the substitute server 503, and makes the portable media 3-1 memorize contents with the use conditions of contents. The receiving agent 732 of the contents manager 725 receives the use conditions of contents, and contents from the substitute server 503.
[0140] The key information receiving agent 726 receives URL which specifies the key server 21-1 which supplies the contents key corresponding to contents, or 21-2 from the shop server 23-1 or 23-2. The contents information receiving agent 727 receives URL which specifies the content ID which specifies desired contents and the contents server 22-1 which supplies desired contents, or 22-2 from the shop server 23-1 or 23-2.
[0141] The format manager 713 transforms into a predetermined method the coding method and cipher system of contents which were downloaded from the contents server 22-1 or 22-2 through the substitute server 503, respectively. The format manager 713 consists of a system discernment program 728, a format conversion program 729, etc.
[0142] The system discernment program 728 is a program for the download place of contents to identify whether it is a server 5-1 or it is a server 5-2. The format conversion program 729 changes the coding method and cipher system of contents.
[0143] Next, the configuration of the substitute server 503 is explained. The substitute server 503 performs LCM514 for servers, and the IP communications program 751.
[0144] LCM514 for servers contains the license manager 761, the sequence manager 762, etc.

[0145] The license manager 761 includes further the server authentication program 781 which attests the key server 21-1 or 21-2, PD authentication program 782 which attests the telephone one apparatus terminal 501.
[0146] The sequence manager 762 includes the key manager 771, the contents manager 772, the system discernment program 773, etc.
[0147] The key manager 771 includes the key distribution program 784 which distributes the contents key further received through the key receiving agent 783 which receives 21-2 to the key server 21-1 or a contents key through a communication network 4, and the communication network 4 to the telephone one apparatus terminal 501.
[0148] The contents manager 772 includes the contents distribution program 786 which distributes the contents which received further through the contents receiving agent 785 which receives 22-2 to the contents server 22-1 or contents through a communication network 4, and the communication network 4 to the telephone one apparatus terminal 501.
[0149] The system discernment program 773 is a program for the download place of contents to identify whether it is a server 5-1 or it is a server 5-2 based on the content ID supplied from the telephone one apparatus terminal 501.
[0150] The IP communications program 751 is a program for including procedures, such as HTTP787 and Wap788, and communicating with a server 5-1, 5-2, or the telephone one apparatus terminal 501 through a communication network 4.
[0151] Next, the telephone one apparatus terminal 501 explains the processing which downloads contents with reference to the flow chart of drawing 11 and drawing 12 from a server 5-1. In step S2101, the PHS/IMT communications program 703 of the telephone one apparatus terminal 501 establishes the public line network 31 and connection. In step S2201, the earth station which the public line network 31 does not illustrate establishes the telephone one apparatus terminal 501 and connection.
[0152] In step S2102, the ISP connection program 702 of the telephone one apparatus terminal 501 establishes ISP32 and connection through connection between the telephone one apparatus terminal 501 and the public line network 31. In step S2301, ISP32 establishes the telephone one apparatus terminal 501 and connection through connection between the telephone one apparatus terminal 501 and the public line network 31.
[0153] Processing with the subsequent telephone one apparatus terminals 501, and the key server 21-1, the contents server 22-1, the shop server 23-1 or the substitute server 503 is performed through connection between the telephone one apparatus terminal 501 and ISP32.
[0154] In step S2103, the IP communications program 701 of the telephone one apparatus terminal 501 establishes the shop server 23-1 and IP communication link. In step S2401, the IP communications program 124 of the shop server 23-1 establishes the telephone one apparatus terminal 501 and IP communication link.
[0155] In step S2402, the perusal program 123 of the shop server 23-1 transmits the digital data for perusal (for selection of contents) to the telephone one apparatus terminal 501 through a communication network 4. The browser program which the telephone one apparatus terminal 501 does not illustrate displays the text or image corresponding to the received digital data on a display 606, and a user is made to peruse it in step S2104. Moreover, by streaming playback of contents, the browser

program of the telephone one apparatus terminal 501 makes the voice playback section 607 reproduce contents, make a user try listening, or it makes the perusal program 123 of the shop server 23-1 search desired contents by the keyword, and displays the result on a display 606.
[0156] Processing of step S2402 and step S2104 is repeated until it determines the contents which a user purchases corresponding to a demand of the user of the telephone one apparatus terminal 501.
[0157] In step S2105, the browser program of the telephone one apparatus terminal 501 transmits a purchase request to the shop server 23-1 through a communication network 4. In step S2403, the perusal program 123 of the shop server 23-1 receives the purchase request transmitted from the telephone one apparatus terminal 501.
[0158] In step S2404, the contents information transmitting program 122 of the shop server 23-1 transmits the contents information containing the content ID for specifying URL of the contents server 22-1 which distributes contents, and contents corresponding to the purchase request which received by processing of step S2403 etc. to the telephone one apparatus terminal 501 through a communication network 4. In step S2106, the contents information receiving agent 727 of the telephone one apparatus terminal 501 receives the contents information which the shop server 23-1 transmitted.
[0159] In step S2405, the key information transmitting program 121 of the shop server 23-1 transmits key information, such as URL of the key server 21-1 which distributes the contents key of the contents corresponding to the purchase request which received by processing of step S2403, to the telephone one apparatus terminal 501 through a communication network 4. In step S2107, the key information receiving agent 726 of the telephone one apparatus terminal 501 receives the key information which the shop server 23-1 transmitted.
[0160] In step S2108, the IP communications program 701 of the telephone one apparatus terminal 501 establishes the substitute server 503 and IP communication link based on URL of the substitute server 503 currently recorded beforehand. In step S2501, the IP communications program 751 of the substitute server 503 establishes the telephone one apparatus terminal 501 and IP communication link.
[0161] In step S2109, the server authentication program 722 of the license manager 711 of the telephone one apparatus terminal 501 attests the substitute server 503. In step S2502, PD authentication program 782 of the license manager 761 of the substitute server 503 attests the telephone one apparatus terminal 501.
[0162] Processing of the mutual recognition of the telephone one apparatus terminal 501 and the substitute server 503 in step S2109 and step S2502 is processing of authentication of a challenge response method, and as compared with processing of the mutual recognition of the key server 21-1 and personal computer 1 in step S112 and step S602, there are few amounts of operations and it can be quickly performed also with little arithmetic proficiency or storage capacity. The telephone one apparatus terminal 501 and the substitute server 503 are the same operations, and generate and share a key from a response temporarily, respectively.
[0163] When processing of the authentication in step S2109 and step S2502 goes wrong, the processing to which the telephone one apparatus terminal 501 downloads contents is ended without downloading contents (when judged with the partner of authentication not being just).

[0164] In step S2110, the contents manager 725 of the telephone one apparatus terminal 501 transmits content ID to the substitute server 503. In step S2503, the substitute server 503 receives the content ID which the telephone one apparatus terminal 501 transmitted. In step S2111, the key manager 724 of the telephone one apparatus terminal 501 transmits the key information received by processing of step S2107 to the substitute server 503. In step S2504, the substitute server 503 receives the key information which the telephone one apparatus terminal 501 transmitted.
[0165] In step S2505, the system discernment program 773 of the substitute server 503 identifies that the download place of contents and a contents key is a server 5-1 based on the content ID which received by processing of step S2503.
[0166] In addition, the telephone one apparatus terminal 501 transmits URL of the contents server 22-1 with content ID, and you may make it the substitute server 503 receive URL of the contents server 22-1 with content ID in step S2503 in step S2110.
[0167] In step S2506, the IP communications program 751 of the substitute server 503 establishes the contents server 22-1 and IP communication link based on the result of discernment of processing of step S2505. In step S2601, the IP communications program 193 of the contents server 22-1 establishes the substitute server 503 and IP communication link.
[0168] In step S2507, the contents manager 772 of the substitute server 503 transmits the content ID acquired by processing of step S2503 to the contents server 22-1 through a communication network 4. In step S2602, the contents server 22-1 receives the content ID which the substitute server 503 transmitted. In step S2603, the contents distribution program 192 of the contents server 22-1 reads the contents (enciphered) corresponding to the content ID which received at step S2602 from the contents preservation program 191, and distributes them to the substitute server 503 through a communication network 4.
[0169] In step S2508, the receiving agent 785 of the contents manager 772 of the substitute server 503 receives the contents which the contents server 22-1 transmitted.
[0170] In step S2509, the IP communications program 751 of the substitute server 503 establishes the key server 21-1 and IP communication link based on the result of discernment of processing of step S2505. In step S2701, the IP communications program 155 of the key server 21-1 establishes the substitute server 503 and IP communication link.
[0171] In step S2510, the server authentication program 781 of the license manager 761 of the substitute server 503 attests the key server 21-1. In step S2702, the authentication program 151 of the key server 21-1 attests the substitute server 503.
[0172] For example, the master key KMSS is beforehand memorized by the key server 21-1, and ID of the individual key KPCC and the substitute server 503 is beforehand memorized by the substitute server 503. The master key KMCC is further memorized beforehand by the substitute server 503, and ID and the individual key KPSS of the key server 21-1 are memorized by the key server 21-1.
[0173] The key server 21-1 receives supply of ID of the substitute server 503 to the substitute server 503, applies a Hash Function to the master key KMSS which the ID and themselves have, and generates the same key as the individual key KPCC of the substitute server 503.

[0174] The substitute server 503 receives supply of ID of the key server 21-1 to the key server 21-1, applies a Hash Function to the master key KMCC which the ID and themselves have, and generates the same key as the individual key KPSS of the key server 21-1. A common individual key will be shared between doing in this way by both the substitute server 503 and the key server 21-1. A key is generated temporarily [ still more temporary ] using these individual keys.
[0175] Processing is ended when processing of the authentication in step S2510 or step S2702 goes wrong (when judged with the partner of authentication not being just).
[0176] In step S2511, the key manager 771 of the substitute server 503 transmits the content ID acquired by processing of step S2503 to the key server 21-1. In step S2703, the key server 21-1 receives the content ID which the substitute server 503 transmitted. In step S2704, the key distribution program 152 of the key server 21-1 reads the contents key which the key preservation program 153 matches with content ID, and is saved, and transmits the contents key (enciphered with the key temporarily which is shared between the key server 21-1 and the substitute server 503) to the substitute server 503 through a communication network 4. In step S2512, the key receiving agent 783 of the key manager 771 of the substitute server 503 receives the contents key which the key server 21-1 transmitted.
[0177] In step S2513, the key distribution program 784 of the key manager 771 of the substitute server 503 is enciphered with a key temporarily which decodes with a key the contents key received by processing of step S2512 temporarily which is shared between the key server 21-1 and the substitute server 503, and shares it between the telephone one apparatus terminal 501 and the substitute server 503, and the contents key enciphered is transmitted to the telephone one apparatus terminal 501 through a communication network 4. In step S2112, the receiving agent 731 of the key manager 724 of the telephone one apparatus terminal 501 receives the contents key which the substitute server 503 transmitted. The key manager 724 is decoded with a key temporarily which shares a contents key between the telephone one apparatus terminal 501 and the substitute server 503, is supplied to the key manager 102 of the portable media 3-1, and makes the key manager 102 memorize a contents key.
[0178] In step S2514, the contents distribution program 786 of the contents manager 772 of the substitute server 503 transmits the contents enciphered to the telephone one apparatus terminal 501 through a communication network 4. In step S2113, the receiving agent 732 of the contents manager 725 of the telephone one apparatus terminal 501 receives the contents which the substitute server 503 transmitted.
[0179] In step S2114, the PHS/IMT communications program 703 of the telephone one apparatus terminal 501 cuts connection with the public line network 31. In step S2202, the earth station which the public line network 31 does not illustrate cuts the telephone one apparatus terminal 501 and connection.
[0180] In step S2115, the format manager 713 of the telephone one apparatus terminal 501 changes a format of the contents which received by processing of step S2113. The contents manager 725 supplies the contents which changed the format to the portable media 3-1 through an interface 609, makes the contents manager 103 memorize contents, and ends processing.
[0181] Next, the telephone one apparatus terminal 501 explains the processing which downloads contents with reference to the flow chart of drawing 13 and drawing 14 from

a server 5-2. Processing of step S3101 thru/or step S3504 is performed by a server 5-2 and the list by the IP communications program 701, the ISP connection program 702, the PHS/IMT communications program 703, and the download program 712, and since it is the same as that of processing of step S2101 thru/or step S2504, the explanation is omitted, respectively.

[0182] In step S3505, the system discernment program 773 of the substitute server 503 identifies that the download place of contents and a contents key is a server 5-2 based on the content ID which received by processing of step S3503.

[0183] In step S3506, the IP communications program 751 of the substitute server 503 establishes the key server 21-2 and IP communication link based on the result of processing of discernment of step S3505. In step S3701, the key server 21-2 establishes the substitute server 503 and IP communication link.

[0184] In step S3507, the server authentication program 781 of the substitute server 503 attests the key server 21-2. In step S3702, the key server 21-2 attests the substitute server 503.

[0185] Processing of step S3507 and step S3702 is the same processing as processing of step S2510 and step S2702.

[0186] Processing is ended when processing of the authentication in step S3507 or step S3702 goes wrong (when judged with the partner of authentication not being just).

[0187] In step S3508, the key manager 771 of the substitute server 503 transmits the content ID acquired by processing of step S3503 to the key server 21-2. In step S3703, the key server 21-2 receives the content ID which the substitute server 503 transmitted. In step S3704, the key server 21-2 reads the contents key which matches with content ID and is saved, and transmits the contents key (enciphered with the key temporarily which is shared between the key server 21-2 and the substitute server 503) to the substitute server 503 through a communication network 4. In step S3509, the key receiving agent 783 of the key manager 771 of the substitute server 503 receives the contents key which the key server 21-2 transmitted.

[0188] In step S3510, the IP communications program 751 of the substitute server 503 establishes the contents server 22-2 and IP communication link based on the result of processing of discernment of step S3505. In step S3601, the contents server 22-2 establishes the substitute server 503 and IP communication link.

[0189] In step S3511, the contents manager 772 of the substitute server 503 transmits the content ID acquired by processing of step S3503 to the contents server 22-2 through a communication network 4. In step S3602, the contents server 22-2 receives the content ID which the substitute server 503 transmitted. In step S3603, the contents server 22-2 reads the contents (enciphered) corresponding to the content ID which received at step S3602, and distributes them to the substitute server 503 through a communication network 4.

[0190] In step S3512, the receiving agent 785 of the contents manager 772 of the substitute server 503 receives the contents which the contents server 22-2 transmitted.

[0191] Since processing of step S3512 thru/or step S3115 is the same as processing of step S2513 thru/or step S2115, the explanation is omitted.

[0192] As mentioned above, in any case, it is the same procedure (for example, contents are received after receiving a contents key), and the telephone one apparatus terminal 501 can receive contents and a contents key, also when downloading contents

and a contents key from a server 5-1 by minding the substitute server 503, and also when downloading contents and a contents key from a server 5-2.
[0193] Moreover, the procedure explained with reference to the flow chart of drawing 11 thru/or drawing 14 can shorten time amount which the telephone one apparatus terminal 501 has connected to the public line network 31 as compared with the processing (it explains with reference to the flow chart of drawing 16 and drawing 17 ) whose substitute server 503 mentioned later changes the coding method and cipher system of contents.
[0194] Next, with reference to drawing 15 , the configuration of other functions of the digital data transmission system of this application is explained. The same number as the case of drawing 10 is given to the same part as the case of a configuration of that drawing 10 explained, and the explanation is omitted.
[0195] The telephone one apparatus terminal 501 shown in drawing 15 does not have the format manager 713.
[0196] In addition to the license manager 761 and the sequence manager 762, LCM514 for servers of the substitute server 503 shown in drawing 15 contains the format manager 801.
[0197] The format manager 801 transforms into a predetermined method the coding method and cipher system of contents which were downloaded from the contents server 22-1 or 22-2, respectively. The format manager 801 consists of a system discernment program 811 and a format conversion program 812.
[0198] The system discernment program 811 is a program for the download place of contents to identify whether it is a server 5-1 or it is a server 5-2. The format conversion program 812 changes the coding method and cipher system of contents.
[0199] Next, the telephone one apparatus terminal 501 and the substitute server 503 which show the configuration explain to drawing 15 the processing which downloads contents with reference to the flow chart of drawing 16 and drawing 17 from a server 5-2.
[0200] Since processing of step S4101 thru/or step S4512 is the same as processing of step S3101 thru/or step S3512 respectively, the explanation is omitted.
[0201] In step S4512, the format manager 801 of the substitute server 503 changes a format of the contents which received by processing of step S4512.
[0202] In step S4514, the key distribution program 784 of the key manager 771 of the substitute server 503 is enciphered with a key temporarily which decodes with a key the contents key received by processing of step S4509 temporarily which is shared between the key server 21-2 and the substitute server 503, and shares it between the telephone one apparatus terminal 501 and the substitute server 503, and the contents key enciphered is transmitted to the telephone one apparatus terminal 501 through a communication network 4. In step S4112, the receiving agent 731 of the key manager 724 of the telephone one apparatus terminal 501 receives the contents key which the substitute server 503 transmitted. The key manager 724 is decoded with a key temporarily which shares a contents key between the telephone one apparatus terminal 501 and the substitute server 503, is supplied to the key manager 102 of the portable media 3-1, and makes the key manager 102 memorize a contents key.
[0203] In step S4515, the contents distribution program 786 of the contents manager 772 of the substitute server 503 transmits the contents enciphered to the telephone one apparatus terminal 501 through a communication network 4. In step S4113, the

receiving agent 732 of the contents manager 725 of the telephone one apparatus terminal 501 receives the contents which the substitute server 503 transmitted. The contents manager 725 supplies the contents (the format is changed) which received to the portable media 3-1 through an interface 609, and makes the contents manager 103 memorize contents.

[0204] In step S4114, the PHS/IMT communications program 703 of the telephone one apparatus terminal 501 cuts connection with the public line network 31. In step S4202, the earth station which the public line network 31 does not illustrate cuts the telephone one apparatus terminal 501 and connection, and processing is ended.

[0205] In addition, after the substitute server 503 receives contents from a server 5-1, the processing which receives contents and a contents key from a server 5-1 serves as the procedure of receiving a contents key from a server 5-1, and is performed similarly.

[0206] Thus, the substitute server 503 can change the coding method and cipher system of contents which were received from a server 5-1 or 5-2, and can also supply them to the telephone one apparatus terminal 501. In this case, it becomes unnecessary programming [ which changes the coding method and cipher system of contents ] the telephone one apparatus terminal 501. Therefore, the telephone one apparatus terminal 501 can perform processing which receives contents quickly also with smaller arithmetic proficiency or storage capacity as compared with the case where it is shown in drawing 10 .

[0207] Moreover, although it explained that contents were data of musical sound, the data of not only the data of musical sound but a static image, the data of a dynamic image, the data of a text, or a program may be used.

[0208] In addition, although the telephone one apparatus terminal 501 or the personal computer 502 explained that contents were downloaded, you may make it the telephone one apparatus terminal 501 or not only the personal computer 502 but a portable telephone, PDA (Personal DigitalAssistant), a digital video cassette recorder with an image pick-up function with communication facility, electronic notebook equipment with communication facility, or a pocket mold personal computer etc. download contents.

[0209] Moreover, although it explained that the telephone one apparatus terminal 501 communicated by PHS or IMT, you may make it communicate not only in PHS or IMT but in W-CDMA (Code Division Multiple Access), satellite communication, satellite broadcasting service, PSTN (Public Switched telephone network), xDSL (x Digital Subscriber Line) and ISDN (Integrated Services Digital Network), or a private network etc.

[0210] Although a series of processings mentioned above can also be performed by hardware, they can also be performed with software. When performing a series of processings with software, the program which constitutes the software is installed in a general-purpose personal computer etc. from a program storing medium possible [ performing various kinds of functions ] by installing the computer built into the hardware of dedication, or various kinds of programs.

[0211] The program storing medium which stores the program which is installed in a computer and made into the condition which can be performed by computer As shown in drawing 8 or drawing 9 , a magnetic disk 641 or a magnetic disk 681 (all contain a floppy disk), an optical disk 642 or an optical disk 682 (any -- CD-ROM (Compact Disc-Read Only Memory) --) DVD (Digital Versatile Disc) is included. A magneto-optic disk

643 or a magneto-optic disk 683 (all contain MD (Mini-Disc)), Or it is constituted by the package media which consist of semiconductor memory 644 or semiconductor memory 684, ROM602 in which a program is stored temporarily or permanently or ROM652, HDD661, etc. Storing of the program to a program storing medium is performed through the communications department 608 or the communications department 663 using the communication media of cables or wireless, such as a Local Area Network, the Internet, and digital satellite broadcasting, if needed.

[0212] In addition, in this specification, even if the processing serially performed in accordance with the sequence that the step which describes the program stored in a program storing medium was indicated is not of course necessarily processed serially, it is a juxtaposition thing also including the processing performed according to an individual.

[0213] Moreover, in this specification, a system expresses the whole equipment constituted by two or more equipments.

[0214]

[Effect of the Invention] According to information offer equipment according to claim 1, the information offer approach according to claim 3, and the program storing medium according to claim 4 The 1st information processor is attested and the 2nd information processor or 3rd information processor is attested. The reception of data which specifies the data which specify the 2nd information processor as the Request to Send of the contents and the key from the 1st information processor and a list, or the 3rd information processor is controlled. When the data which specify the 2nd information processor are received, in the procedure corresponding to the 2nd information processor While transmitting the Request to Send of contents and a key to the 2nd information processor When contents and a key are received from the 2nd information processor and the data which specify the 3rd information processor are received, in the procedure corresponding to the 3rd information processor While transmitting the Request to Send of contents and a key to the 3rd information processor Since a communication link is controlled to receive contents and a key from the 3rd information processor and the contents to the 1st information processor and transmission of a key were controlled The contents and the key which are supplied in the procedure in which the throughputs of the 1st information processor differ that it is small can be received now.

[0215] According to an information processor according to claim 5, the information processing approach according to claim 6, and the program storing medium according to claim 7 The 1st information offer equipment is attested. The contents to the 1st information offer equipment, and the Request to Send of a key, The data which specify the 2nd information offer equipment which provides a list with contents and a key, And transmission of either of the data which specifies the 3rd information offer equipment which offers contents and a key is controlled. Since the 1st information offer equipment receives offer from the 2nd information offer equipment or the 3rd information offer equipment and reception of the contents and the key which were transmitted was controlled, the contents and the key which are supplied in the procedure in which throughputs differ that it is small can be received.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the configuration of the conventional digital data transmission system.
[Drawing 2] It is drawing showing the configuration of the function of the conventional digital data transmission system.
[Drawing 3] It is a flow chart explaining the conventional processing which a personal computer 1 downloads contents from a server 5-1, and checks out to the portable device 2.
[Drawing 4] It is a flow chart explaining the conventional processing which a personal computer 1 downloads contents from a server 5-1, and checks out to the portable device 2.
[Drawing 5] It is a flow chart explaining the conventional processing which a personal computer 1 downloads contents from a server 5-2, and checks out to the portable device 2.
[Drawing 6] It is a flow chart explaining the conventional processing which a personal computer 1 downloads contents from a server 5-2, and checks out to the portable device 2.
[Drawing 7] It is drawing showing the gestalt of 1 operation of the digital data transmission system concerning this invention.
[Drawing 8] It is drawing explaining the configuration of the telephone one apparatus terminal 501.
[Drawing 9] It is drawing explaining the configuration of the substitute server 503.
[Drawing 10] It is drawing explaining the configuration of the function of the digital data transmission system of this application.
[Drawing 11] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-1.
[Drawing 12] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-1.
[Drawing 13] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-2.
[Drawing 14] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-2.
[Drawing 15] It is drawing explaining the configuration of other functions of the digital data transmission system of this application.
[Drawing 16] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-2.
[Drawing 17] The telephone one apparatus terminal 501 is a flow chart explaining the processing which downloads contents from a server 5-2.
[Description of Notations]
501 Telephone One Apparatus Terminal 503 substitute server 511 A display operator guidance program, 512 LCM for clients 514 LCM for servers, 601 CPU 602 ROM 603 RAM 608 communications department, 641 Magnetic disk 642 optical disk 643 A magneto-optic disk and 644 semiconductor memory 651 CPU 652 ROM 653 RAM 663 Communications department 681 Magnetic disk 682 An optical disk and 683 Magneto-optic disk 684 Semiconductor memory